E-Learning
E-Safety AND ICT for Learning Policy

Author: AP Director of Science
Date adopted by Governors/Academy:
Date of last review/amendment: September 2017
Date of next review: September 2020

Peter 2: Verse 17-23. Treat everyone you meet with Dignity. Love your spiritual family. Revere (worship) God. This is the kind of life you've been invited into, the kind of life Christ lived. He never did one thing wrong. Not once said anything amiss. They called Him every name in the book and He said nothing back. He suffered in silence, content to let God set things right.

Introduction

Our Academy Vision is "Living Well Together with Dignity, Faith and Hope. We aspire to take dignified decisions and afford dignity to all members of our community, regardless of background or circumstance. Our position as a Voluntary Aided Church Academy means that the Christian faith has a central role in all our actions and decisions. We strive for excellence in all that we do, enabling our students to transform their lives and to hope for happy and successful futures.

At All Saints Academy, our vision is "Living Well Together in Dignity, Faith and Hope and this translates into our everyday practice. The value of dignity is particularly relevant when we consider the use of e-learning, social media and ICT as we want to promote a community which is safe and accessible for all.

All Saints Academy Dunstable is committed to ensuring opportunities and access for all and values the abilities and achievements of all our students. We recognise the value of parents/carers in supporting their children and will look to engage them in planning to meet the needs of individuals.

In order to reflect our vision, this policy is made up of three key issues related to e-learning, e-safety and best practice ensuring that the use of technologies by staff and students are maximised and used within the guidelines of the law.

The statutory curriculum expects students to learn how to locate, retrieve and exchange information using IT. In delivering the curriculum, teachers need to plan for and make use of communications technology, for example, web-based resources and email. Access to life-long learning and employment increasingly requires use of technology and students need to develop life skills in their use and we see e-learning as a significant tool to enhance teaching and learning at All Saints Academy Dunstable and enable students to flourish and reach their potential.

Procedures

E-learning may be defined as any form of instruction where computer technology, and other technologies, are used and applied to facilitate learning.

Peter 2: Verse 17-23. Treat everyone you meet with Dignity. Love your spiritual family. Revere (worship) God. This is the kind of life you've been invited into, the kind of life Christ lived. He never did one thing wrong. Not once said anything amiss. They called Him every name in the book and He said nothing back. He suffered in silence, content to let God set things right.

E-Learning provision may be:

1. Web supported

This form of e-learning is used to provide students with easy access to basic information such as teacher notes, practice exam questions, module handbooks, PowerPoint presentations, etc. It runs in parallel with face-to-face teaching, which continues as the more prominent mode of delivery. Online participation would not usually be assessed either, though students may receive feedback from teachers on homework/coursework progress etc.

2. Web-dependent

This form of e-learning contains all the elements of the above with online participation by students being required, and may be assessed. Online content would therefore be more substantial than notes or PowerPoint presentations and will have been developed using a range of e-learning activities (e-tivities) and exercises. An example of this could be collaborative learning, e.g. peer, group or learning sets could be used and teacher feedback could be considerable.

3. Fully Online

Students interact exclusively online and generally they would not attend face-to-face classes. Interaction between teachers and fellow students would be conducted within a VLE (Virtual Learning Environment). Such courses/modules would be supported by a strongly tested and developed e-learning infrastructure.

In developing a working framework for e-learning within the Academy, each of the above is regarded, for the purposes of this policy, as a separate and therefore planned developmental stage in policy implementation. At the time of writing this policy it is expected that for most students, face-to-face teaching will be their most familiar instructional experience.

E-safety

E-safety depends on effective practice at a number of different levels:

- Responsible IT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure Academy network design and use.
- Safe and secure broadband.
- National Education Network standards and specifications.

To ensure the safe use of technology and enhance our hospitable community and to fulfil our vision of Living Well Together, staff and students within the Academy will read and sign IT and Internet Acceptable Use Policies, which can be found in the resources section.

Peter 2: Verse 17-23. Treat everyone you meet with Dignity. Love your spiritual family. Revere (worship) God. This is the kind of life you've been invited into, the kind of life Christ lived. He never did one thing wrong. Not once said anything amiss. They called Him every name in the book and He said nothing back. He suffered in silence, content to let God set things right.

The security and safe use of related systems within technological devices are stated below:

1. Information system security
- Academy IT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the local authority.

2. Email communication is a vital tool and we want staff and students to have faith that they will be treated with mutual trust and dignity in these communications.
- Students may only use approved email accounts on the Academy system.
- Students must immediately tell a teacher if they receive offensive email.
- Students must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.
- Email sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on Academy headed paper.
- The forwarding of chain letters is not permitted.
- All email correspondence should be written with dignity and respect for the addressee.

3. Published content and the Academy website
- The contact details on the website should be the Academy address, email and telephone number. Staff or students' personal information will not be published.
- The Principal (or nominee) will take overall editorial responsibility and ensure that content is accurate and appropriate.

4. Publishing students' images and work
- Photographs that include students will be selected carefully to ensure trust, faith and embodies our vision of Living Well Together. They will not deliberately enable individual students to be clearly identified.
- Students' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the Academy website.
- Work can only be published with the permission of the student and parents.

5. Social networking and personal publishing. Staffs, Students and Parents have faith that we will ensure their e-safety. To enable this
- The Academy will block/filter access to social networking sites.

Peter 2: Verse 17-23. Treat everyone you meet with Dignity. Love your spiritual family. Revere (worship) God. This is the kind of life you've been invited into, the kind of life Christ lived. He never did one thing wrong. Not once said anything amiss. They called Him every name in the book and He said nothing back. He suffered in silence, content to let God set things right.

- Newsgroups will be blocked unless a specific use is approved.
- Students will be advised never to give out personal details of any kind which may identify them or their location.
- Students must not place personal photos on any social network space.
- Students should be advised on security and encouraged to set passwords, deny access to unknown individuals and know how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.

6. Managing filtering

- The Academy will work in partnership with the Internet Service Provider to ensure systems to protect students are reviewed and improved.
- If staff or students discover an unsuitable site, it must be reported to the Network Manager.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

7. Managing videoconferencing

- Video conferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Students should ask permission from the supervising teacher before making or answering a video conference call.
- Video conferencing will be appropriately supervised for the students' age group.

8. Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in the Academy is allowed.
- Mobile phones will not be used during lessons or formal Academy time. The sending of abusive or inappropriate text messages is forbidden.
- Internet enabled wearable devices are not to be used during lessons, exams or formal Academy time.

9. Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. All members of All Saints Academy community have faith that their data will be protected.

Assessing risks

The Academy will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will

never appear on an Academy computer. The Academy cannot accept liability for the material accessed, or any consequences of Internet access. The Academy will periodically audit IT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

Handling e-safety complaints

Complaints of Internet misuse will be dealt with dignity by a senior member of staff.

Any complaint about staff misuse must be referred to the Principal.

- Complaints of a child protection nature must be dealt with in accordance with Academy child protection procedures.
- Students and parents will be informed of the complaints procedure.
- Discussions will be held with the Police Youth Crime Reduction Officer, where appropriate to establish procedures for handling potentially illegal issues.

Communicating the e-safety policy

- E-safety rules will be posted in all networked rooms.
- Students will be informed that network and Internet use will be monitored.
- All staff will be given the Academy e-safety policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Respect for the Academy, discretion and professional conduct is essential.
- Staff who manage filtering systems or monitor IT use will be supervised by senior management and have clear procedures for reporting issues.
- Parents' attention will be drawn to the Academy e-safety policy in newsletters, the Academy prospectus and on the Academy website.

Monitoring, Evaluation and Review

The Governing Body has delegated to the Principal the responsibility for reviewing the implementation and effectiveness of this policy. The Governing Body will approve all major changes to this policy. The policy will be promoted and published throughout the Academy.

Related Academy Policies:

- Anti-bullying Policy
- Behaviour Management Policy
- Child Protection Policy
- Data Protection Policy
- Exclusions Policy
- Fixed Asset Procedure and Accounting Policy

Peter 2: Verse 17-23. Treat everyone you meet with Dignity. Love your spiritual family. Revere (worship) God. This is the kind of life you've been invited into, the kind of life Christ lived. He never did one thing wrong. Not once said anything amiss. They called Him every name in the book and He said nothing back. He suffered in silence, content to let God set things right.

- In-house Communications Policy
- Photographs and Video Policy
- Race Equality Policy
- Safeguarding and Promoting Students' Welfare Policy
- Staff Code of Conduct & Disciplinary Policy
- Social Media Policy

RESOURCES

Peter 2: Verse 17-23. Treat everyone you meet with Dignity. Love your spiritual family. Revere (worship) God. This is the kind of life you've been invited into, the kind of life Christ lived. He never did one thing wrong. Not once said anything amiss. They called Him every name in the book and He said nothing back. He suffered in silence, content to let God set things right.

IT Acceptable Use Policy – Summary - Staff

Equipment

- Always get permission from the Network Manager before installing, attempting to install or storing programs of any type on the computers. Evidence of licence will be required.
- Do not eat or drink in the vicinity of the IT equipment or IT suites.
- All maintenance should be carried out by IT support staff.
- Protect the computers from spillages by eating or drinking well away from the IT equipment or IT suites.

Security and Privacy

- Protect your work by keeping your password to yourself; do not use someone else's logon name or password without the specific permission of the Principal.
- To protect yourself and the systems, you should respect the security on the computers; attempting to bypass or alter the settings may put you or your work at risk.
- Your files and communications will be monitored to ensure that you are using the system responsibly.

Email

- If you receive an email containing material of a violent, dangerous, racist, or inappropriate content, always report such messages to your line manager. The sending of an email containing content likely to be unsuitable for Academies is strictly forbidden.
- The @allsaintsAcademydunstable.org account provided by IT support should be used for all communications with staff, students, parents and other agencies.

Licences

- All Software, Music, Images, Videos MUST have a licence that covers use in the Academy.
- No ITunes or other music, files, images can be attached to the Academy network at any time unless a licence can be produced.

Peter 2: Verse 17-23. Treat everyone you meet with Dignity. Love your spiritual family. Revere (worship) God. This is the kind of life you've been invited into, the kind of life Christ lived. He never did one thing wrong. Not once said anything amiss. They called Him every name in the book and He said nothing back. He suffered in silence, content to let God set things right.

Internet

Users shall not visit unsuitable Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- pornography (including child pornography)
- promoting discrimination of any kind
- promoting racial or religious hatred
- promoting illegal acts
- any other information which may be offensive to other users in the Academy community.

Incidents which appear to involve deliberate access to websites, newsgroups and online groups that contain the following material will be reported to the police:

- images of child abuse (images of children, apparently under 16 years old) involved in sexual activity or posed to be sexually provocative
- adult material that potentially breaches the Obscene Publications Act in the UK
- criminally racist material in the UK.

If inappropriate material is accessed accidentally, users should immediately report this to the ASAD Network Manager so that this can be taken into account in monitoring.

Users shall not:

- Use the ASAD facilities for running a private business.
- Enter into any personal transaction that involves ASAD or the Local Authority in any way.
- Visit sites that might be defamatory or incur liability on the part of ASAD or the Local Authority or adversely impact on the image of ASAD.
- Upload, download, or otherwise transmit (make, produce or distribute) commercial software or any copyrighted materials belonging to third parties outside of ASAD, or to ASAD itself.
- Reveal or publicise confidential or proprietary information, which includes but is not limited to:
    - financial information
    - personal information
    - databases and the information contained therein
    - computer/network access codes

Peter 2: Verse 17-23. Treat everyone you meet with Dignity. Love your spiritual family. Revere (worship) God. This is the kind of life you've been invited into, the kind of life Christ lived. He never did one thing wrong. Not once said anything amiss. They called Him every name in the book and He said nothing back. He suffered in silence, content to let God set things right.

    - business relationships.

- Intentionally interfere with the normal operation of the Internet connection, including the propagation of computer viruses and sustained high volume network traffic (sending or receiving of large files or sending and receiving of large numbers of small files or any activity that causes network congestion) that substantially hinders others in their use of the Internet.

Monitoring

- The Academy reserves the right to monitor electronically all activity on its network and any device attached to it. This includes computers, laptops, flash drives, MP3s etc whether they belong to the Academy or not.

Please read this document carefully. If you violate these provisions you may be subject to disciplinary action. Additional action may be taken by the Academy.

On evidence provided by ASAD, an employee may be disciplined. At the same time, if a user's conduct and/or action(s) are illegal, the user may become personally liable in some circumstances.

I agree to the full terms & Conditions as clearly depicted in the ***E-Learning E-Safety and ICT for Learning Policy*** and specifically in relation the pages 7 through to 13.

Name: …….
(Please ensure your name is printed clearly)

Date: ……

Signed: …….

Peter 2: Verse 17-23. Treat everyone you meet with Dignity. Love your spiritual family. Revere (worship) God. This is the kind of life you've been invited into, the kind of life Christ lived. He never did one thing wrong. Not once said anything amiss. They called Him every name in the book and He said nothing back. He suffered in silence, content to let God set things right.

IT Acceptable Use Policy – Summary - Student

Equipment

- Never attempt to install or storing programs of any type on the computers.
- All maintenance should be carried out by IT support staff.
- Do not eat or drink in the vicinity of the IT equipment or IT suites.
- Turn off any equipment when you have finished using it unless you are instructed otherwise by a member of staff

Security and Privacy

- Protect your work by keeping your password to yourself; never use someone else's logon name or password.
- If you find a computer that another user has forgotten to log off from then inform a member of staff.
- To protect yourself and the systems, you should respect the security on the computers; attempting to bypass or alter the settings is unacceptable behaviour.
- Your files and communications will be monitored to ensure that you are using the system responsibly.

Email

- If you receive an email containing material of a violent, dangerous, racist, or inappropriate content, always report such messages to a member of staff. The sending of an email containing content likely to be unsuitable for young people or Academies is strictly forbidden.
- The @allsaintsAcademydunstable.org account provided by IT support should be used for all communications with Academy staff and for communicating with other students for Academy work purposes.

Peter 2: Verse 17-23. Treat everyone you meet with Dignity. Love your spiritual family. Revere (worship) God. This is the kind of life you've been invited into, the kind of life Christ lived. He never did one thing wrong. Not once said anything amiss. They called Him every name in the book and He said nothing back. He suffered in silence, content to let God set things right.

- Webmail such as hotmail should not be used at all in the Academy.
- The use of email for bullying will be investigated and dealt with in accordance with the Academy bullying policy.

Licences

- All Software, Music, Images, Videos MUST have a licence that covers use in the Academy.
- A copy of this must be given to Network Manager.
- No iTunes or other music, files, images can be attached to the Academy network at any time unless a licence can be produced.

Internet

Users shall not visit unsuitable Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- pornography (including child pornography)
- promoting discrimination of any kind
- promoting racial or religious hatred
- promoting illegal acts
- any other information which may be offensive to other users in the Academy community.

Incidents which appear to involve deliberate access to websites, newsgroups and online groups that contain the following material will be reported to the police:

- images of child abuse (images of children, apparently under 16 years old) involved in sexual activity or posed to be sexually provocative
- adult material that potentially breaches the Obscene Publications Act in the UK
- Criminally racist material in the UK.

If inappropriate material is accessed accidentally, users should immediately report this to the ASAD Network Manager so that this can be taken into account in monitoring.

Users shall not:

- Use the ASAD facilities for running a private business.
- Enter into any personal transaction that involves ASAD or the Local Authority in any way.
- Visit sites that might be defamatory or incur liability on the part of ASAD or the Local Authority or adversely impact on the image of ASAD.

Peter 2: Verse 17-23. Treat everyone you meet with Dignity. Love your spiritual family. Revere (worship) God. This is the kind of life you've been invited into, the kind of life Christ lived. He never did one thing wrong. Not once said anything amiss. They called Him every name in the book and He said nothing back. He suffered in silence, content to let God set things right.

- Upload, download, or otherwise transmit (make, produce or distribute) commercial software or any copyrighted materials belonging to third parties outside of ASAD, or to ASAD itself.
- Reveal or publicise confidential or proprietary information, which includes but is not limited to:
    - financial information
    - personal information
    - databases and the information contained therein
    - computer/network access codes
    - business relationships.
- Intentionally interfere with the normal operation of the Internet connection, including the propagation of computer viruses and sustained high volume network traffic (sending or receiving of large files or sending and receiving of large numbers of small files or any activity that causes network congestion) that substantially hinders others in their use of the Internet.

Monitoring

- The Academy reserves the right to monitor electronically all activity on its network and any device attached to it. This includes computers, laptops, flash drives, MP3s etc whether they belong to the Academy or not.

Please read this document carefully. If you violate these provisions you may be subject to disciplinary action. Additional action may be taken by the Academy.

I agree to the full terms & Conditions as clearly depicted in the ***E-Learning E-Safety and ICT for Learning Policy*** and specifically in relation the pages 14 through to 18.

Name: …… Date: ……
(Please ensure your name is printed clearly)

Tutor Group: ……

Signed: ……

Peter 2: Verse 17-23. Treat everyone you meet with Dignity. Love your spiritual family. Revere (worship) God. This is the kind of life you've been invited into, the kind of life Christ lived. He never did one thing wrong. Not once said anything amiss. They called Him every name in the book and He said nothing back. He suffered in silence, content to let God set things right.

Peter 2: Verse 17-23. Treat everyone you meet with Dignity. Love your spiritual family. Revere (worship) God. This is the kind of life you've been invited into, the kind of life Christ lived. He never did one thing wrong. Not once said anything amiss. They called Him every name in the book and He said nothing back. He suffered in silence, content to let God set things right.

COMPUTER SECURITY

1. Physical Equipment Security
   - Where possible, computer equipment will be sited so as to reduce the risk of unauthorised access and damage.
   - The details of all computer equipment will be recorded in the official inventory record together with relevant serial numbers.
   - Computer hardware will be appropriately security marked.
   - A record will be kept of any computer equipment taken off site. The removal of equipment from the Academy's premises must be authorised by the Principal.
   - The officer responsible for physical equipment security is the Network Manager.

2. Backup Procedures
   - All data held on the Academy's computer system will be backed every evening the Academy is open. Personal data held on individual computers will NOT be backed up.
   - Backups are rotated every two weeks and will be clearly labelled.
   - A year-end backup of financial data will be taken and retained using separate disks each year.
   - ALL backups will be stored in the fireproof safe in the Manager's office when not in use.
   - The officer responsible for backup procedures for the System Network is the Network Manager.

3. Virus Detection
   - All computers will have virus detection software installed within their start-up procedures. The Network Manager updates the software regularly.
   - Any disks of uncertain origin must be scanned for viruses before use.
   - The use of unlicenced software is prohibited.
   - Any perceived virus attach should be immediately reported to the Network Manager.
   - The officer responsible for virus detection procedures is the Network Manager.

4. Software Controls
   - All software is maintained by the Academy and must be properly owned by the Academy. Software may only be used in accordance with the licence agreement. Personally owned software WILL be removed.
   - The Network Manager will hold all licences and system disks so that they are aware of all the software installed in Academy. The system disks are stored in the locked IT room cupboard.

Peter 2: Verse 17-23. Treat everyone you meet with Dignity. Love your spiritual family. Revere (worship) God. This is the kind of life you've been invited into, the kind of life Christ lived. He never did one thing wrong. Not once said anything amiss. They called Him every name in the book and He said nothing back. He suffered in silence, content to let God set things right.

- The Network Manager will keep an inventory of all software maintained on the Academy's computers, together with relevant serial numbers.
- Access to software will be restricted to authorised staff.
- The Network Manager is the only person who may issue passwords and amend access levels.
- Users of the Academy's computer system will be issued with individual passwords.
- It should be ensured that passwords are kept confidential.
- Staff should LOCK the computer system before leaving any PCs unattended.
- When staff leave, their accounts will be disabled immediately by the Systems Manager.
- Any suspected breach of security will be immediately reported to the Principal.
- The officer responsible for software control is the Systems Manager.

5. Legal Obligations
   - All staff should be made aware of the requirements and their responsibilities in relation to the following legal statutes:
     1. 1984 Data Protection Act
     2. 1986 Copyright, Design and Patents Act
     3. 1990 Computer Misuse Act.

6. Acquisition, Maintenance and Disposal of Hardware
   - The Principal has overall responsibility for the acquisition, maintenance and disposal of equipment.
   - ALL IT related software and equipment purchases MUST go through the Network Manager to be able to compare "best prices" and "best value".
   - Official orders will be used for purchases.
   - The write off and disposal of equipment should be authorised by the Governing Body and the Principal.
   - Acquisition and disposal of equipment must be in accordance with the Financial Regulations for Academies.

7. User Training
   - Users should receive appropriate training in the correct use of the Academy's IT facilities including use of software packages and security arrangement.

8. Disaster Recovery
   - There will be adequate arrangements in place for disaster recovery including emergency procedures, manual fallback plans and resumption of procedures.

Peter 2: Verse 17-23. Treat everyone you meet with Dignity. Love your spiritual family. Revere (worship) God. This is the kind of life you've been invited into, the kind of life Christ lived. He never did one thing wrong. Not once said anything amiss. They called Him every name in the book and He said nothing back. He suffered in silence, content to let God set things right.

- The officer responsible for disaster recovery is the Network Manager as the backup of the Academy network includes the server, financial systems and students' administration.

9. Internet Access
   - There will be adequate procedures in place to ensure that access to the Internet is appropriate for the person accessing it and the necessary blocks and security measures are in place to prevent misuse.
   - The officer responsible for maintaining the Internet access is the Network Manager.

10. Key Personnel
    - Network Manager – responsible for maintaining and securing the Academy's main network and server systems. In their absence, support will be provided by his department.
    - Assistant Vice Principal (Finance and Operations) – responsibility for the management and backup of the Academy's financial software package. In their absence, the day-to-day operation of the department would be continued by the Finance Manager. Additional support would be requested from the LA's Academy Finance Department as part of the Bursary Service and via the Academy's advisory team, to ensure continued financial administration and the maintenance of financial control.
    - Attendance Officer – responsibility for the management and backup of Academy's student and attendance software data. Other personnel within the Admin Department would assume duties in their absence.