Joseph Leckie Academy

Joseph Leckie Academy

E-Safety Policy

Approved by Governors
14/02/2018

Introduction and Aims

The purpose of this policy is to establish the ground rules we have in Joseph Leckie Academy for using ICT equipment and the Internet.

New technologies have become integral to the lives of children and young people in today's society, both within educational establishments and in their lives outside school. The Internet and other digital/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. This e-safety policy will help to ensure safe and appropriate use. The use of these exciting and innovative tools in the Academy 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 or 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 read and used in conjunction with other Academy policies; specifically Anti-Bullying, Behaviour, Child Protection and Mobile Phone Use (in the Positive Behaviour Policy).

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

Roles & Responsibilities

This section outlines the roles and responsibilities for e-safety of individuals and groups within the Academy.

Governors

Governors are responsible for the approval of the e-safety policy and for reviewing the effectiveness of the policy. A named member of the Governing Body, has taken on the role of E-Safety Governor. The role of the E-Safety Governor will include:

- Meetings with the ICT and E-Safety Coordinator
- Regular monitoring of e-safety incident logs
- Monitoring of filtering/change control logs
- Reporting to relevant Governors and/or committee(s) meetings.

Principal & ~~Senior~~ Leadership Team (~~S~~LT)

The Principal is responsible for ensuring:

- The safety (including e-safety) of all members of the Academy, although the day to day responsibility for e-safety may be delegated to the E-Safety Coordinator
- Adequate training is provided
- Effective monitoring systems are set up
- That relevant procedure in the event of an e-safety allegation are known and understood.
- Establishing and reviewing the Academy's e-safety policies and documents (in conjunction with E-Safety Co-ordinator)
- The Academy's Designated Child Protection Officers should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise through the use of IT.

E-Safety Coordinator

The E-Safety Coordinator takes day to day responsibility for e-safety issues and has a leading role in:

- Liaising with staff, ICT Technical staff, E-Safety Governor and ~~S~~LT on all issues related to e-safety;
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place;
- Providing training and advice for staff;
- Receiving reports of e-safety incidents and creates a log of incidents to inform future e-safety developments;
- Co-ordinating and reviewing e-safety education programme in school

Head of ICT/ICT Coordinator

The ICT Coordinator is responsible for ensuring that:

- The school's ICT infrastructure is secure and meets e-safety technical requirements
- The school's password policy is adhered to
- The Academy uses Policy Central to filter specific words and phrases are updated on a regular basis and that its implementation is not the sole responsibility of any single person
- Co-ordinator keeps up to date with e-safety technical information

- The use of the school's ICT infrastructure (network, remote access, e-mail, VLE etc.) is regularly monitored in order that any misuse or attempted misuse can be reported to the E-Safety Coordinator and/or SLT for investigation/action/sanction.

Currently Joseph Leckie Academy engages the services of Policy Central for day-to-day monitoring of words/sites used by users on the Academy's PCs and laptops. The Principal/Assistant Principal therefore has an additional responsibility to ensure that the support team adhere to the above e-safety measures during the course of their activities and are aware of Security and Acceptable Usage Policy.

Teaching & Support Staff

In addition to elements covered in the Staff Accessible Usage Policy (AUP), all teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current Academy e-safety policy and practices
- They have read, understood and signed the Academy's Staff Acceptable Usage Policy (AUP)
- E-safety issues are embedded in all aspects of the curriculum and other Academy activities
- Students understand and follow the Academy's e-safety and acceptable usage policies
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright legislation
- They monitor ICT activity in lessons and extracurricular activities
- In lessons where Internet use is pre-planned, 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.

Students (to an age appropriate level)

- Are responsible for using the Academy's ICT systems in accordance with the Student Acceptable Usage Policy, which they will be required to sign before being given access to academy systems. Parents/carers will be required to read through and sign alongside their child's signature. (Student planner)
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the Academy's e-safety policy also covers their actions out of school, if related to their membership of the Academy.

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 Academy will therefore take opportunities to help parents understand these issues. Parents and carers will be responsible for:

- Endorsing (by signature) the Student Acceptable Usage Policy.
- Accessing the school website in accordance with the relevant Academy Acceptable Usage Policy.

Community Users

Community Users who access school ICT systems/website/Learning Platform as part of the Extended School provision will be expected to sign a Volunteer User AUP (see Appendix 6) before being provided with access to the Academy's ICT systems.

Education and Training

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

- A planned e-safety programme is provided as part of the form tutor and assembly programme and is regularly revisited in Information Technology and other lessons across the curriculum – this programme covers both the use of ICT and new technologies in ~~school~~ and outside of school.
- Students are taught in lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of the information.
- Students are helped to understand the need for the Student AUP and encouraged to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside of the Academy.
- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- Staff act as good role models in their use of ICT, the Internet and mobile devices.

Acceptable Usage Policy

- **Parents/carers** will be required to read through and sign alongside their child's signature, helping to ensure their children understand the rules
- **Staff and regular visitors** to the Academy have an AUP that they must read through and sign to indicate understanding of the rules.

Copyright

- Students to be taught an appropriate understanding of research skills and the need to avoid plagiarism and uphold copyright regulations- staff to monitor this.
- Students are taught, appropriate to their age, to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- If using a search engine for images – staff / students should open the selected image and go to it's website to check for copyright.

Staff Training

- E-safety coordinator ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- A planned programme of e-safety training is available to all **staff**. An audit of the e-safety training needs of all staff will be carried out regularly.
- All new **staff** receive e-safety training as part of their induction programme, ensuring that they fully understand the school E-Safety policy, Acceptable Usage and Child Protection Policies.
- The **E-Safety Coordinator/LT link** will receive regular updates through Local Authority and/or other information/training sessions and by reviewing guidance documents released.
- **Governors** are invited to take part in e-safety training and awareness sessions, with particular importance for those who are members of any committee or working group involved in ICT, e-safety, health and safety or child protection.

Communication

Email

- Digital communications with students (e-mail, VLE or text.) should be on a professional level and only carried out using official Academy systems
- The Academy's e-mail should be used if communicating with students
- Under no circumstances should staff contact students, parents/carers or conduct any Academy business using personal e-mail addresses.
- Academy e-mail is not to be used for personal use. Staff can use their own email in the Academy (before, after school and during lunchtimes when not working with children) – but not for contact with parents/ students.

Mobile Phones

- **Academy** mobile phones only should be used to contact parents/carers/students when on Academy business with students off site. Staff should not use personal mobile devices unless they have had permission from the Principal.
- **Staff** should not use personal mobile phones in the Academy during working hours when in contact with students.
- Students should adhere to the rules and guidelines set out in the Behaviour Policy regarding mobile phone use in the Academy.

Social Networking Sites

Young people will not be allowed on social networking sites whilst using the Academy equipment.; at home it is the parents' responsibility, but they should be aware that it is illegal for children under the age of 13 to be on certain social networking sites.

- **Staff** should not access social networking sites on Academy equipment whilst at work or at home. Staff should access these sites using personal equipment.
- **Staff** users should not reveal names of staff, students, parents/carers or any other member of the Academy on any social networking site or blog**.**
- **Students/Parents/carers** should be aware the Academy will investigate misuse of social networking if it impacts on the well-being of other students, staff members or stakeholders.
- If inappropriate comments are placed on social networking sites about the Academy or Academy staff then advice would be sought from the relevant agencies, including the police if necessary.
- Students in the KS3 curriculum will be taught about e-safety on social networking sites as we accept some may use it outside of school.

Digital Images

- The Academy record of parental permissions granted/not granted must be adhered to when taking images of our students. A list is published to all staff on a termly basis, but can also be obtained from the Academy's Information System.
- Under no circumstances should images be taken using privately owned equipment without the express permission of the Principal or LT.

Websites

- In lessons where Internet use is pre-planned, 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.
- Staff will preview any recommended sites before use.
- "Open" searches (e.g. "find images/ information on...") are discouraged when working with younger students who may misinterpret information.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by staff. **Parents** will be advised to supervise any further research.
- **All** users must observe copyright of materials published on the Internet.
- Teachers will carry out a risk assessment regarding which students are allowed access to the internet with minimal supervision. Minimal supervision means regular checking of the students on the internet by the member of staff setting the task. All staff are aware that if they pass students working on the internet that they have a role in checking what is being viewed. Students are also aware that all internet use at school is tracked and logged.
- The Academy only allows the E-Safety Co-ordinator and members of LT access to Internet logs.

Passwords

Staff

- Passwords or encryption keys should not be recorded on paper or in an unprotected file
- Passwords should be changed at least every 3 months
- Users should not use the same password on multiple systems or attempt to "synchronise" passwords across systems

Students

- Should only let Academy staff know the ICT passwords.
- Should inform staff immediately if passwords are traced or forgotten. All staff are able to access the network to allow students to change passwords

Monitoring

Any member of staff employed by the Academy who comes across an e-safety issue does not investigate any further but immediately reports it to the e-safety co-ordinator and impounds the equipment. If the concern involves the E-Safety co-ordinator then the member of staff should report the issue to the Principal or members of the LT.

Incident Reporting

Any e-safety incidents must immediately be reported to the Principal (if a member of staff) or the E-Safety Coordinator (if a student) who will investigate further following e-safety and safeguarding policies and guidance.

Responding to incidents of misuse

It is hoped that all members of the Academy 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. The Academy Principal will deal with staff misuse.

Appendix 1

Acceptable ICT Use Policy – Students

Student / Pupil Acceptable Use Policy Agreement

I understand that I must use the Academy ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the Academy will monitor my use of the ICT systems, email and other digital communications.
- I will not share my username or password, nor will I try to use any other person's username and password.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line.
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the Academy ICT systems for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the Academy has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the Academy:

- I will only use my personal hand held / external devices (mobile phones / USB devices etc) in Academy if I have permission. I understand that, if I do use my own devices in the Academy, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I am aware that damage to personal hand held devices isn't the responsibility of the Academy unless permission for use was granted.
  I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any attachments to emails, unless I know and trust the person / organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.

- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of the Academy:

- I understand that the Academy also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of the Academy and where they involve my membership of the Academy community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the Academy network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please note agreement of this Acceptable Use Agreement is necessary to continue. If you do not agree, access will not be granted to the Academy ICT systems.

Acceptable Internet Use Policy – Staff and Volunteers

Staff/Volunteers Acceptable Use Policy Agreement

I understand that I must use the Academy ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users including students.

For my own personal safety:

- • I understand that the Academy has the right to monitor all aspects of its IT systems (computers, internet, emails, social network use) including personal devices when connected to the Academy network and WiFi to ensure that the Academy IT systems are not compromised, used inappropriately and for our responsibilities with respect to Safeguarding and Prevent.
- • I will not share my username or password, nor will I try to use any other person's username and password.
- • I will not disclose or share personal information about myself or others when on-line.
- • I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- • I will ensure that when using the Academy systems and devices and any personal devices which connect to the Academy network/WiFi or are used for Academy business, that I will comply with the following policies:

  - Staff Code of Conduct
  - Data Protection Policy & Data Protection Act 2018 (GDPR)
  - E-Safety Policy
  - Whistleblowing Policy

I will act as I expect others to act toward me:

- • I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- • I will not take or distribute images of anyone without consent

I recognise that the Academy has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the Academy:

- • I am aware that damage to personal hand held devices isn't the responsibility of the Academy unless permission for use was granted.
- • I will immediately report any damage or faults involving equipment or software, however this may have happened to ICT support and the line manager of the department.
- • I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- • I will not open any attachments to emails, unless I know and trust the person / organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.
- • I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings without first consulting the ICT Support Department.
- • I understand that I should only store Academy related resources/files on the network areas, and not use these areas for storage of personal files.

When using the internet for research or recreation, I recognise that:

- • I should ensure that I have permission to use the original work of others in my own work
- • Where work is protected by copyright, I will not try to download copies (including music and videos)

- • When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of the Academy:

- • I understand that the Academy also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of the Academy and where they involve my membership of the Academy community (examples would be cyber-bullying, misuse of images or personal information).
- • I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action as per the staff code of conduct and in the event of illegal activities involvement of the police.

Please note: Whilst using Academy ICT systems you should also abide by the policies listed above, these are available on the Academy website.

Please note: Agreement of this Acceptable Use Agreement is necessary to continue. If you do not agree, access will not be granted to the Academy ICT systems.