



Joseph Swan Academy

**ICT, Internet and Acceptable Use Policy
(Incorporating electronic and online safety and
mobile device use)**

2017 – 2018

To be reviewed September 2018

Contents

	Page
Introduction	3
ICT – General Conditions of Use	3
ICT Access Policy	3
ICT Access Control	4
Internet and email Acceptable Use	5
Internet Filtering arrangements	7
E Commerce arrangements	7
Email Use - General Regulations	8
Email Content	8
Use of email for non-work related purposes	9
Anti – virus arrangements	10
Online Safety Policy	11
Mobile Phones & electronic devices policy	14
Appendix 1 Employee Acceptable Use Arrangement	
Appendix 2 Letter to Parent/Carer	
Appendix 3 Code of Conduct for use of the Academy’s E-Learning Facilities	
Appendix 4 Student Electronic Learning Code of Conduct Agreement	

ICT, Internet and email Acceptable Use Policy

Introduction:

Joseph Swan Academy encourages employees and students to use ICT to progress learning and promote the efficient leadership and management of the Academy.

To ensure that the network and systems run smoothly, all users must accept responsibility for their actions and abide by the regulations/protocols associated with this policy.

This policy has been approved by the Governing Body and failure to follow these rules may lead to disciplinary action for employees (and suspension of students) and possible civil/criminal proceedings.

ICT - General Conditions of Use:

Access to ICT, Internet and email will be made available to employees and students, when the appropriate agreements have been signed. Employees will note the Academy's ICT provision is intended to be used for activities directly related to Academy business. Whilst there is provision for employees to use these facilities for personal use; such use during working hours must be minimal and rare.

Loan of ICT Equipment:

Any person wishing to borrow ICT equipment must register it's use with iSupport. All users must ensure only appropriate internet sites are accessed whilst equipment is in their possession and all appropriate steps must be taken to ensure the safe return to Academy.

All items are borrowed at the employee's/student's own risk and items must be protected against loss, theft, unauthorised access and damage.

Any user becoming aware of any irregular use of ICT should inform the Head Teacher.

ICT Access Policy:

All employees and students will have controlled access to the Academy network They will also be granted monitored and filtered access to the internet and email.

Temporary employees may be given access to the system and this policy also applies to them.

Any attempt, by any user, to access ICT resources, other than through the channels and access routes provided and intended by the Academy, is not acceptable.

- The ICT network is password protected
- All users must ensure that their password is not shared with anyone else

- Users are responsible for the material accessed and stored using their ID and password
- Activity on the Academy's network is monitored for all users
- Passwords are to be renewed every 30 days

Administrator rights are held by members of the iSupport Team; in addition to this, a copy is to be held in Academy safe. The Leadership Team will have access to this.

If a member of staff leaves their work station the computer must be locked.

Requests to have software added to the network must be made to the iSupport Team. Requests for the purchase of software to be added to the network must be discussed with the iSupport or designated Academy Leadership Team member.

Requests for changes to access, for students, to allow them to complete specific curriculum tasks must be made by the Subject Leader to iSupport, giving 1 weeks advance notice. Any student who is in breach of the code of conduct could have their access suspended. The Leadership Team member responsible for ICT is the only employee who is able to sanction this.

Any employee wishing to purchase ICT Hardware must first discuss their requirements with the iSupport and/or Leadership Team Member with ICT responsibility, for approval. All orders must then be submitted via iSupport for approval.

In line with Academy procedures, all ICT equipment must be security coded before being issued. This is the responsibility of the iSupport.

Internet and Email Acceptable Use:

Employees need to be aware that Internet and email use will be monitored and if misuse is indicated then, under RIPA, individual users may be identified and their personal browsing and email activity monitored (in real- time or retrospectively), reviewed and investigated.

The following list gives examples of 'misuse' but it is not an exhaustive list;

- Access or attempting to access or transmit information or images that are obscene, sexually explicit, racist or defamatory or which depict violent or criminal acts
- Access or attempting to access peer to peer or file sharing networks or sites
- Gambling
- Use for commercial gain
- Chat room access
- Instant messaging or web messaging
- Creating and maintaining a personal website
- Downloading or Uploading materials which are not relevant to the work of the Academy

In view of the potential risks with Internet and email use, the individual responsibility for all employees to both understand and follow the regulations cannot be over emphasised.

Users should also be aware that for some forms of infringement, personal liability could lead to civil proceedings or prosecution.

Internet Use – General regulations;

Internet users must:

- Have signed the Internet User Agreement
- Only use their own personal identifiers
- Not disclose their personal password to others, nor use it to allow another person access to Internet facilities, whether the other person is authorised themselves or not
- During designated working hours all employees are reminded that any Internet activity should be related to their work. If employees wish to use the Internet for personal business this would normally take place outside of working hours and not to access inappropriate sites. The management of the Academy accept that, occasionally, employees may wish to access internet sites for personal purposes, during working hours, but expect such use to be minimal and rare
- Inform iSupport of any web address that the Internet user considers inappropriate
- Not infringe any copyright, licence, patent or similar legal issue in copying or downloading material during web browsing
- Not apply any downloaded software material to any computer without prior consultation with, and written approval from iSupport
- Notify the Head Teacher of any irregular use of systems of facilities at the earliest opportunity

Training and Support for Users:

- Support for Internet and email is available from the iSupport Team
- Requests for training should be made to the employee responsible for CPD within the Academy

Internet Filtering Arrangements:

The Academy's Internet Service on the network is filtered in an attempt to avoid access to inappropriate Internet content. However, errors in site filtering can occur.

iSupport should be notified of any legitimate web site that has been blocked. As soon as the legitimate nature of the site is agreed, the block will be lifted and the Internet users will be notified accordingly.

Requests to have websites enabled for students must be emailed to iSupport, giving 24hrs notice.

If any web site content is found to be inappropriate, the Internet user must inform the iSupport, as soon as practicable. The site will then be blocked.

E-Commerce Arrangements

The Internet provides E-Commerce facilities to allow the procurement of online purchases for Academy business purposes.

Where appropriate authorisation has been granted, personal cash or credit facilities can be used to complete on-line Academy purchases with subsequent reimbursement through General Purposes Account and petty cash systems. This should only be used as a last resort. The Academy cannot guarantee the security or reliability of any E-Commerce web site; therefore, Academy users should not rely on the Academy or Governing Body to take responsibility for any problems arising for the use of such facilities.

Problems relating to the use of E-Commerce facilities should be reported to iSupport and Business Manager.

The guidelines relating to E-Commerce will be kept under review and subject to revision in the light of changes in Internet technology and E-Commerce regulation and security.

Email use – General Regulations.

Email users should note that the same risks (for example, legal action as a result of defamatory comments or harassment made in email) can, and do apply equally to email sent inside the Academy via its Gmail, as to external emails sent via the Internet.

General Rules for email use

Email users must:

- Have signed Internet and Email User Agreement
- Only use their own personal identities
- Not disclose their personal password to others, nor use it to allow another person access to email facilities, whether the other person is themselves authorised or not
- Ensure that email messages are appropriately addressed to identify the name and designation of the email user and Academy name. Decorative graphics must not be used in the email messages as they can adversely affect the Academy system
- Not open or execute any email file attachment if the content of the attachment is unknown or uncertain
- Notify iSupport and or Head Teacher of any apparent irregular use of email systems or facilities at the earliest opportunity

Email content

All external email messages transmitted through the Academy's systems will be archived automatically and retained for the statutory period of time.

Email can be used for formal Academy business purposes and general communications (for example, transmission of messages, arranging meetings) and in many cases replacing normal postal services and telephone use.

As such email users should ensure that their personal management of incoming and outgoing email mirror existing practices and procedures within the Academy for the handling of written correspondence and telephone communications.

Email users must:

- Not transmit any sensitive, confidential information or data that could, by accident or design, cause detriment to the Academy
- Ensure that the content of transmitted email messages, (including file attachments), could not be seen as expressing libellous or defamatory opinion or comment, fact or otherwise, which may cause detriment to the Academy
- Ensure that email messages involving personal data or licensed or copyrighted material do not infringe laws on Data Protection, copyright, license or patent restrictions
- Ensure that any personal opinions or comments expressed are compatible with Academy policy
- Ensure that the content of any transmitted email messages, (including file attachments), will not reasonably be perceived as intended to cause, offence, harassment or inconvenience to the receiver, or delay, or disruption of any kind to their computer system
- Ensure the content of any transmitted email messages, (including file attachments), will not be reasonably constructed in any way as entering the Academy into any kind of agreements or contractual obligation
- Must not use own personal email address for any Academy business, especially when corresponding with students and parents

Use of Email for non-work related purposes

Email may be used for limited personal, non-work related purposes. However email users must:

- Ensure personal use of email is minimal and content is brief
- Excessive amounts of personal email can adversely affect the Academy's system
- Not use email for the purposes of casual social communication or any kind of personal organised business
- Not send file attachments with personal emails
- Not send or receive personal emails on behalf of others
- Not send or forward 'chain email'
- Ensure that, personal emails are normally sent out of working hours

Anti-virus Arrangements

- Although the Academy's email provision is secured by up to date versions of anti-virus software to filter incoming email, there is still a risk from the newest viruses that appear. Email users are therefore advised to maintain a degree of caution about incoming email messages, even when the sender's name is recognised
- Particular care should be taken with unsolicited email messages, with or without a file attachment that entices the user to open them, or warn of a computer virus
- Employees must not forward, to colleagues, any email attachment that they receive which purports to warn of virus or similar computer problems. They should instead notify iSupport at the earliest opportunity
- File attachments often present a virus threat. Where unsolicited mail is received, email users must not open any attachment without prior consultation with iSupport

Handling Electronic information

Electronic information of a sensitive or privileged nature must not be taken from the Academy site unless it is on an encrypted electronic device.

Failure to Adhere to Regulations/Misuse of ICT, Internet and Email Systems

A breach of the regulations may be detrimental to the Academy (it's Governors, Employees or Students).

Academy Governors may become vicariously liable for the actions of its employees.

Additionally, for certain types of infringement, users may become personally responsible and liable to prosecution or civil proceedings from outside the Academy Governors jurisdiction.

Where these regulations are disregarded, to the extent that the offending action causes detriment to the Academy, then Academy Governors may take disciplinary action, including dismissal, against any offending user concerned. Students contravening these regulations will be subject to normal Academy disciplinary proceedings.

In the event of downloading or distributing information, from the internet, by an employee, the Academy's findings may have to be shared with police for any potential criminal activity to be investigated.

Joseph Swan Academy Online Safety Policy

This policy is linked to:

- ICT Acceptable use Policy
- Safeguarding Policy.
- Mobile Phone + New Technologies Policy

Online Safety Awareness

An education programme on electronic safety will be delivered to all students to raise their awareness and importance of safe and responsible Internet and New Technologies use. This programme will include a clear explanation of the Academy rules on electronic safety.

This programme will be delivered via Tutorial periods, Assemblies and ICT Lessons.

- See Appendix 1 Electronic Safety Strategy for all Students.

This programme will be continuously monitored and revised to accommodate emerging needs.

Parents and carers will be regularly reminded via the Academy Newsletters, Progress Days and the Academy Website of the importance of electronic safety

Systems security

The security of the Academy information systems will be reviewed regularly.

- Virus protection will be updated regularly.
- The ICT System Manager will review system capacity regularly
- The Academy will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via an Academy computer. The Academy cannot accept liability for the material accessed, or any consequences resulting from Internet use.
- The Academy will block access to social networking sites.

Students' images

Images that include students will be selected carefully and will not 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 images of students are electronically published.

How will electronic safety complaints be handled?

Sanctions within the Academy discipline policy include:

- Interview/counselling by the head of year; informing parents or carers; removal of Internet or computer access for a period
- Serious complaints may be reported to the appropriate authorities

How will emerging technologies be managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in Academy is allowed

Online Safety Guidance – Staff

The following guidance for all staff is aimed at protecting both staff and students.

If, as a member of staff you are concerned about any aspect of electronic safety then you need to consult with a member of the Academy Leadership Team.

- Staff must not give students their personal mobile phone number. Staff must not give students their own personal email addresses
- If staff chose to join social networking sites they are strongly advised to adopt high levels of security
- When using social media staff must not publish anything which negatively reflects on the Academy or its employees
- Staff must not invite students to be their friends, or accept invitations from students, on social network sites
- Staff must have the 'Bluetooth' function on personal mobiles is secure

Mobile Phones and Electronic Devices Policy

Rationale:

Mobile Phones and Electronic Device have become an important part of our modern lifestyle. The Academy understands there are times when possession of a mobile phone can provide a sense of safety and security while travelling to and from Academy, or when staying late at the Academy to attend extra-curricular activities.

Mobile Phones and Electronic Device are multi-faceted including video, photography, voice recording, games and music and, in the correct context, many of these 'tools' can be invaluable in our new technological world and students should be encouraged to use these facilities positively to enhance learning presentation and understanding. However, if abused, these devices can interfere with learning in the Academy, can invade privacy and can be used to hold information which may be interpreted as pornographic, bullying and for criminal purposes.

Mobile phones and electronic devices are expensive and students bring their equipment to Academy at their own risk; the Academy will not be liable for loss or damage to such devices.

Staff bringing their own portable electronic device into Academy must ensure that it does not contain any offensive or compromising material. Information of a sensitive or privileged nature must not be stored on a member of staff's own personal laptop or digital storage device unless the Academy's iSupport Team have encrypted it.

Students

Unless otherwise directed by a member of staff to support their learning, students' mobile phones and electronic devices should be switched off. Phones should **not** be on silent or vibrate as they can cause distraction

Students should **not** be allowed to listen to music on their personal devices during a lesson at any time.

Any student who has their Mobile Phones and/or Electronic Device visible in Academy will have it removed and must collect from their Year office at the end of the Academy day.

Sixth Form students can use Mobile Phones and Electronic Device but only in Sixth Form Areas.

Mobile Phones and Electronic Devices should never be used to take photographs of staff. If a student is found using their Mobile Phone or Electronic Device to take photos of staff then a senior member of staff should be called immediately, who should confiscate the phone and contact parents. Subsequent action will be determined by the specific details of the incident. However, this is likely to be deemed a serious incident and will be dealt with accordingly.

Inappropriate use of Mobile Phones and Electronic Devices by students to take pictures of other students will similarly be treated as a serious offence.

Staff:

- Mobile phones are to be switched off/silent profile during meetings, duties and class sessions.
- Staff must not give out their personal phone number to parents/carers or students
- Staff must ensure that their phones and electronic devices do not contain any inappropriate, offensive or compromising material.

Parents/Carers:

- Parents/Carers will be asked to turn phones off when attending assemblies, performances and meetings so that there is no disruption to the Academy's programmes.



STAFF

ICT, Internet, Email, mobile phone Acceptable Use and Online Safety Agreement

To be completed by all members of staff employed at Joseph Swan Academy.

I have read the ICT, Internet and email Acceptable Use, Mobile Phone and Electronic Devices, and the Online Safety Policies and agree to abide by them:

Name: _____

Signature: _____ Date: _____



Electronic Learning Code of Conduct

Dear Parent/Carer

As part of our curriculum we encourage students to make use of educational resources available on the Internet. Access to the Internet enables students to conduct research and obtain high quality educational resources from, libraries, museums, galleries and other information sources from around the world.

To guard against accidental access to materials which are inappropriate to Joseph Swan Academy students, a filtering service is used. However it is not possible to provide 100% assurance that students might not accidentally come across material which is inappropriate.

Before students are allowed to access the Internet we would like them to discuss the attached Electronic Learning code of Conduct with their parents/carers and then to complete and return the attached form to Tutors.

We believe that the educational benefits to students from access to the Internet, in the form of information resources and opportunities for collaboration, far outweigh the potential disadvantages.

During lesson time staff will guide students towards specific materials and educational resources. Where students are given permission to access the Internet outside lessons they must agree to access only those sites that are appropriate for use in Academy and use the electronic learning resources appropriately.

Yours faithfully

Miss H E Scott
Head Teacher



Code of conduct for use of the Academy's Electronic Learning facilities

This code of conduct applies at all times, in and out of Academy hours, whilst using Academy equipment.

Access to the Internet and an email account will be provided for you to conduct research and communicate with others. This is on the understanding that you agree to follow this code. This code of conduct is not intended to be exhaustive. At all times you should use e-learning resources in an appropriate and responsible manner.

The code You

should:

- Only access sites which are appropriate for use in Academy.
- Be aware that your actions on the Internet may be monitored.
- Always keep your username and password private and secure.
- Be aware that information on an Internet website may be inaccurate or biased. Try to verify the information using other sources.
- Be careful of what you say to other and how you say it. Never give your name, home address, telephone numbers or any personal information about yourself or others to any strangers you may write to or communicate with on the Internet. Never arrange to meet strangers who approach you whilst on the computer; anyone can pretend to be someone else. Someone pretending to be a friend may not have your best interests at heart.
- Treat others as they would expect to be treated, *e.g. show respect and be polite.*
- Always tell your teacher or another adult if you ever see, hear or read anything which makes you feel uncomfortable while using the Internet or email.
- Respect copyright and trademarks. *You cannot use the words or pictures that you see on an Internet site without giving credit to the person that produced the information originally. You must not copy text or pictures from the Internet and hand it in to your teacher as your own work.*
- Check with a teacher before:
 - Downloading files.
 - Completing questionnaires or subscriptions forms.
 - Opening email attachments.

You should not:

- Send, access, store or display offensive messages or pictures
- Send any electronic messages which may contain abusive, threatening, racist or any other inappropriate sentiments/language
- Access any other user's files, emails or personal web space without their permission

Please note:

You should always logout and close your browser when your session has finished.

User areas on the Academy network will be closely monitored and staff may view your files and communications to maintain the system's integrity.

Failure to follow the code may result in loss of access and further disciplinary action may be taken if appropriate. If applicable, external agencies may be involved; certain activities may constitute a criminal offence.



Electronic Learning Code of Conduct Agreement

Student: _____ **Tutor Group:** _____

I have read the Electronic Learning Code of Conduct and I agree to follow it.

Signature: _____ Date: _____

Parent/Carer

As parent/carers, I have read, discussed and explained the Electronic Learning Code of Conduct to my son/daughter. I understand that if he/she fails to follow this code, his/her individual access may be withdrawn and I will be informed.

Parent/Carer Signature: _____ Date: _____

Name (please print): _____ Date: _____

Permission for use of student photographs, work and copyright release

This Academy may produce printed publications and/or an Academy website which may include examples of student's work and/or photographs of students. No child's work will ever be used without his/her permission and we take the issue of child safety very seriously which includes how we use images of students. The Academy has a duty of care towards students, which means we will ensure that it is difficult to identify any individuals who appear in Academy publications this will reduce the risk of inappropriate contact, if images are used in this way.

We ask that parent/carers consent to the Academy publishing their children's work and to the taking and using of photographs and images of their children subject to strict confidentiality of personal information.

I consent to photographs and digital images of the child named above, appearing in printed publications or on the Academy website. I understand that the images will be used only for educational purposes and that the identity of my child will be protected. I also acknowledge that the images may also be used in and distributed in other media, such as CD-ROM, as part of the promotional activities of the Academy. I also consent to examples of my child's work being published on the Academy web site or in other media, subject to strict confidentiality of personal information.

Parent/Carer Signature: _____ Date: _____

Name (please print): _____ Date: _____

For Academy use only:

Date returned: _____