



## **NETWORK AND INTERNET ACCEPTABLE USE**

### **Academy Policy**

Document Title	Network & Internet Acceptable Use Policy
Approved by:	KPJA Governing Body
Approval Date:	January 2019
Review Frequency:	Every three years
Review Date:	January 2022

Network use and access are considered an academy resource. If the academy AUP is not adhered to, access will be withdrawn and appropriate sanctions imposed. The AUP should be read carefully to ensure the conditions of use are accepted and understood before it is signed.

### **Aims**

- The aims of this Acceptable Use Policy are:
- To ensure that staff benefit from the opportunities offered by the academy's IT resources in a safe and effective manner;
- To provide and maintain IT resources for the benefit of all staff and children;
- To encourage staff to use these resources as an aid to effective execution of professional duties and responsibilities;
- To protect the academy's IT infrastructure from misuse and attack;
- To protect and securely maintain Sensitive and Personal Data.

At Kettering Park Junior Academy we understand the responsibility to educate our pupils on eSafety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

This policy covers fixed and mobile internet technologies provided by the academy (such as PCs, laptops, webcams, whiteboards, digital video equipment, iPads etc.)

### **General - Staff**

- The Head teacher reserves the right to monitor use of the network including review of your files and communications, to ensure that you are using the system responsibly.
- Senior staff may be required to access your account/documents in the course of their duties.
- Be aware of your responsibilities to Data Protection and follow the academy Data Protection Policy regarding the use of personal or sensitive information.
- Observe good computer etiquette at all times and never undertake actions that may bring the academy into disrepute. Respect other computer users and neither harass, harm, offend nor insult.
- Always log off at the end of your session so other people are not prevented from using the computer.
- Use the academy network and computers only for educational purposes and those involving the operation of the Academy.
- Computers must not be used for any illegal or disreputable activity out of keeping with the professional duties of staff. This includes:
  - Use of illegally obtained software (i.e. without a valid licence certificate);
  - Deliberate viewing of inappropriate material as files on the computer;
  - Unauthorised copying of software, contrary to the provisions of the Copyright, Designs and Patents Act 1988;
  - Violation of copyright laws concerning the publication of materials;
  - Actions that may contravene the Computer Misuse Act 1990.
- Computer equipment (other than staff issue laptops and iPads) should not be taken off site without formal authorisation of the Head teacher.
- Software must be approved by the Head/IT Lead and must be given to the IT Lead in case proof of ownership is required. Failure to do so may result in that software being withdrawn from use.
- Uploading and downloading of non-approved software is not permitted.
- The system is backed up on a daily basis.

### **Standard Equipment**

- Please be aware that you are accountable for equipment being used by children under your supervision.
- Do not install, or attempt to install hardware of any type on the network without the consulting of the IT Lead.
- Do not connect, or attempt to connect personal mobile equipment (e.g. laptops, Tablets, Mobile Phones, PDAs etc.) to the network without consulting the IT lead.
- Do not damage, disable, tamper with, attempt to dismantle or otherwise cause, or attempt to cause harm to the operation of computers or any IT equipment or associated cabling.
- Always check files brought in on removable media (such as CD-ROMs, Pen/Flash drives) or downloaded from the internet, with antivirus software and only use them if they are found to be clean of viruses. In the event of a suspected virus, inform the IT lead immediately.
- Do not eat or drink within close proximity of IT equipment.

### **Staff Laptops, iPads and Accessories**

- The equipment issued to you remain the property of the academy and is on loan whilst you are employed at the academy.
- Where it is absolutely essential to store sensitive personal information (such as student or staff data) on a laptop, it must only be done under the guidance of the academy Data Protection Policy.
- This equipment should never be left in an unattended car or public place.
- This equipment should be used within the academy at least once a month to receive software patches and antivirus updates. These will be performed automatically. On some occasions the IT lead will ask you to bring in your for some updates.
- The academy IT system does not routinely backup data from laptops. It is your responsibility to do this.

### **Security and Privacy**

1. Protect your work by keeping your password to yourself and be aware that you are responsible for the actions of any other user logged on with your network identity.
2. Change passwords at regular intervals. Should you suspect your network or any other credentials to be compromised, you must change your password and inform the IT Lead immediately.
3. Never use someone else's logon name or password.
4. Never allow children to use your login credentials. Student security privileges are extremely restrictive - for good reason.
5. When leaving a computer unattended, always use the Ctrl/Alt/Del function to lock the screen.
6. Do not attempt to bypass or alter security settings put in place on the networks. They are there to protect you, your work and academy resources.
7. Ensure any sensitive information is kept on an encrypted USB flash drives.
8. Be aware of those around you when viewing confidential or sensitive information. Do not access sensitive information in public places like internet cafes or coffee bars.
9. Any printed 'hard copy' of confidential or sensitive information must be kept securely and shredded when finished with.
10. Do not trespass in other people's folders, work or files.

### **Internet**

- The Internet is provided for you to conduct genuine research and communicate with others. A record is kept of the sites visited by you. Remember that access is a privilege, not a right, and that usage requires responsibility at all times.
- Using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted.

- You are expected to exercise professional conduct when accessing the web - visiting only sites appropriate for viewing in an academy environment.
- Respect the work and ownership rights of people outside the academy, as well as other students or staff. This includes abiding by copyright laws.

### **Email**

- Take care opening attachments or clicking on links in an email. These can contain viruses or other programmes that could cause extensive damage to the network. If in doubt, consult the IT Lead.
- The use of strong language, swearing or aggressive behaviour will not be permitted.
- Emails containing material with violent, dangerous, racist, or inappropriate content must be reported to a relevant member of staff. The sending or receiving of an email containing content likely to be unsuitable for schools is strictly forbidden.
- Sensitive data should never be sent by email.
- Always check the entire email chain to ensure you are not inadvertently sending inappropriate information to third parties or people who should not receive it.
- The academy provides all staff with a professional email account to use for all academy related business, including communications with parents and carers. This allows for email content to be monitored and protects staff from the risk of allegations, malicious emails or inappropriate contact with children and their families.

### **eSafety in the Curriculum**

- The academy provides opportunities within a range of curriculum areas to teach about eSafety.
- Educating pupils on the dangers of technologies that maybe encountered outside Academy is done informally when opportunities arise and as part of the e-Safety curriculum and visit from outside providers to deliver e-safety to children, families and staff on a yearly basis
- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Pupils are taught about copyright and respecting other people's information, images, etc. through discussion, modelling and activities.
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline/ CEOP report abuse button

### **Managing the Internet**

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the network is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

- The children will only have supervised access to Internet
- Staff will preview any recommended sites before use.
- If Internet research is set for homework, it is advised that parents check the sites and supervise the work. Parents will be advised to supervise any further research.

- All users must observe software copyright at all times. It is illegal to copy or distribute academy software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

### **Personal Mobile devices (including phones)**

- The academy allows staff to bring in personal mobile phones and devices for their own use.
- The academy is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any members of the academy community is not allowed.
- Permission must be sought before any image or sound recordings are made on these devices of any member of the academy community.
- Users bringing personal devices into the academy must ensure there is no inappropriate or illegal content on the device.

### **Safe Use of Images**

#### Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misused. We must remember that it is not always appropriate to take or store images of any member of the academy community or public.

The academy informs parents that images may be taken of pupils on academy equipment for use in newsletters, displays and on academy social media sites. We ask that parents let us know if they do not wish their children to be included in such publications.

Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However with the express permission of the Head teacher, images can be taken provided they are transferred immediately and solely to the academy network and deleted from the staff device.

#### Publishing pupil's images and work

On a child's entry to the academy, all parents/guardians will be informed that photos of their children or children's work may be used in the following ways:

- On the academy web site
- Recorded/ transmitted on a video or webcam
- In display material that may be used in the academy's communal areas
- General media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

Parents are asked to let the academy know if they do not wish their child to have photos taken. Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published.

#### Storage of Images

Pupils and staff are not permitted to use personal portable media for storage of images (e.g. USB sticks) without the express permission of the Head teacher

Rights of access to this material are restricted to the teaching staff and pupils within the confines of the Academy network.

Disclaimer: Due to the constant changes taking place within technology, this policy may not contain the most recent developments. We will however, endeavour to add any important issues to the policy on our website.

## Appendix 1



### Agreement for the acceptable use of the internet, e-mails and computers

At Kettering Park Junior Academy we understand the importance and benefits of using computers and the internet to help with children's learning and personal development. However, we also recognise that safeguards need to be in place to ensure children are kept safe at all times.

Please could parents/carers read and discuss this policy with their child. A copy will be available on the school website for reference purposes.

- I will only use IT in school for school purposes.
- I will only use any class e-mail address or any school e-mail address of my own when e-mailing.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not tell other people my password.
- I will only open my own files.
- I will make sure that all IT contact with other children and adults is responsible, polite and sensible.
- I will not send anyone material that could be considered threatening, bullying, offensive or illegal.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out my personal details such as my name, phone number or home address.
- I will be responsible for my behaviour when using IT because I know that these rules are to keep me safe.
- I will not deliberately upload or add any images, video, sounds or text that could upset anyone within the school community.
- I know that my use of IT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my online behaviour or safety.

**Appendix 2**



**Kettering Park Junior Academy**  
**Off-site equipment Agreement**

For the purpose of this document “mobile equipment” will mean laptops, Mobile Phones, iPads and other tablets.

**Ownership**

The mobile equipment remains the property of the academy. Upon leaving your employment, the equipment must be returned in good condition with any personal files removed. Any mobile equipment is subject to audit at any time and must be produced if requested.

**Security**

The equipment is covered by academy insurance if stolen by forced entry to your home. If stolen from your car it is not covered:-

- You will take full responsibility for the physical security of your mobile equipment at all times
- Whilst off-site the mobile equipment will be kept in a secure place. If left in a car, the car will be locked and the equipment out of site.
- In the event of theft/loss you will report this immediately to the Head, School Business Manager and, if necessary, the police. If the equipment is lost or stolen and you are found negligent, you will be asked to make contribution towards replacement.

This policy acts as an agreement between you and Kettering Park Junior Academy in respect of the equipment listed below:-

**Name**.....

**Class/Location**.....

**Laptop Model**.....

**Laptop serial number**.....

**Other mobile equipment i.e. iPad, other tablet, Mobile Phone, etc.**

.....

**Signature**.....

**Date**.....

## Appendix 3

### Academy Mobile Phones

Where a mobile phone has been issued by the academy, it is for **business use only** and at all times will remain the property of the academy. The user(s) will be responsible for its safekeeping, proper use, condition and eventual return to the academy. The user will also be responsible for any cost of repair or replacement other than fair wear and tear. If a replacement is required the Academy will organise this.

A mobile phone is provided primarily to enable the user to do their job, i.e. to keep the academy informed at the earliest opportunity of matters which it needs to know about and to be similarly contactable by the academy. Therefore, it is the user's responsibility to ensure that the mobile phone is kept charged and switched on whilst on duty.

Users should not sign up to text based information services, e.g. RAC traffic alerts, text voting. The use of the internet on Company mobile phones is strictly prohibited, except in the case where specific authorisation has been given by the Head Teacher Smartphone users should only use the internet to access their academy emails and for other essential Academy use.

Unless agreed by the Head Teacher, applications and other programmes may not be downloaded to any Academy mobile phone under any circumstance.

The SIM card from academy mobiles should not be placed into any other mobile, unless to another academy issued mobile phone. Neither should the camera facility be used for anything other than an emergency, e.g. company car accident where evidence may be required.

The academy recognises that users may, **on occasion**, have to make personal calls or send personal text messages during working hours, or outside normal working hours. Where it is deemed that an unreasonable amount of personal calls/text messages have been made using the mobile phone, the academy reserves the right to deduct those costs, either through deduction from pay, or otherwise. The academy may, after formal investigation, take action under the Disciplinary Procedure if such use is excessive or unauthorised. Users will be expected to make payment for private calls made beyond reasonable usage.

If it is found, following investigation, that there has been excessive personal data use, then the user will be asked to reimburse the academy for the cost of this and action may be taken under the Disciplinary Procedure.

The user agrees that upon termination of employment, should they not return the allocated mobile phone, or should the mobile phone be returned in an unsatisfactory condition, the cost of replacement, or a proportional amount of this as decided by the academy, will be deducted from any final monies owing, or the user will otherwise reimburse the academy.

### Use of a Mobile Phone Whilst Driving

The user must ensure they have full control of any vehicle that they are driving at all times. It is an offence to use hand held mobile phones whilst driving or whilst the engine is turned on. The user will be liable for prosecution if they are holding a mobile phone, or any other type of hand held

device to send or receive any sort of data, be it voice, text or pictorial images. The user will be regarded to be driving if they are in charge of a vehicle with its engine running on a public road, even if the vehicle is stationary. It is therefore strictly forbidden for the user to use a hand held mobile phone whilst driving.

A mobile phone may only be used where there is an in-coming call or an out-going voice activated call through a hands free device that is activated without a need to hold the phone at any time, in which case the call should be kept to the shortest possible time and only to effect essential communications. When the phone needs to be operated to make or deal with a call through the hands free device for longer than receiving or giving a short communication, before doing so the user must stop and park the vehicle where it is safe and lawful to do so and with the engine switched off. Whilst driving they must not use the text message facility on the mobile phone, or if available through such a phone, an image facility or internet access.

It should be noted carefully that a breach of the academy's rules on the use of a mobile phone whilst driving may render the user liable to action under the Disciplinary Procedure.

### **Lost or Stolen Mobiles**

The user is responsible at all times for the security of the mobile phone and it should never be left unattended. A PIN number should be used on the mobile to enable voicemails to be picked up. If unsure how to do this, please contact academy Office to speak to the appropriate person for instructions.

If the phone is lost or stolen, this must be reported to academy Office immediately (if during working hours), or if out of hours phone the mobile provider to ensure that the account is stopped and there is no unauthorised usage.

In the event of theft of a mobile phone, the incident must also be reported to the police and an incident number obtained (please provide this number when reporting the loss to academy Office).

The academy reserves the right to claim reimbursement for the cost of the phone, or excess usage charges should the correct procedures not be followed, a user reports repeated loss of their mobile, it is deemed that the user has not taken appropriate measures to safeguard the equipment, or reported the loss thereof (which will be investigated by the academy and judged at its absolute discretion).

### **Monitoring of Usage and Costs**

The academy receives itemised billing for all academy mobile phones and this is monitored on a monthly basis. The billing system identifies all calls, texts and data usage (if appropriate) and the costs related to this, by user, destination, duration, frequency, etc. High or clear personal usage will be reported to Head Teacher for investigation (high usage is defined as usage which falls outside of the normal usage pattern for the individual, or outside of the usage pattern in comparison to other similar users).

If it is found the mobile has been misused, the academy may, after formal investigation, take action under the Disciplinary Procedure.

## **Mobile Phone Use Abroad**

All academy mobile phones are barred from being used abroad unless the network provider has been specifically instructed by the Company. In the event that a bar needs to be lifted, please contact Head Office in order that this may be considered.

It is particularly important on Smartphones to ensure that “data roaming” is switched off for any times other than checking Company emails. “Data roaming” charges from abroad (which includes the Isle of Man and Channel Islands) can result in very high level charges, and if it is found that these have been incurred due to personal use or negligence on the part of the user, then the charges may be passed on to the user.