# ICT Acceptable Use Agreement for Academy Employees

**Overview**

This document is issued for the protection of Ernulf Academy employees and children in their care. Please ensure that you have read this and understand your obligations and responsibilities. Failing to follow this advice and guidance could leave employees vulnerable or lead to more robust action.

It is important to remember that in the case of images, texts, emails and other information the sender no longer has control of the data once sent (and it could potentially be posted in the public domain). As such, the action could be damaging to the sender and to the reputation of the Academy. Remember, once sent, you cannot take it back!

As an employee of the Academy you are expected to behave responsibly and safely and comply with the advice and guidance given in this document.

For the purpose of this document, a device includes:

- Any computer or device issued to an Academy employee for purpose of his/her work
- Any laptop belonging to or connected to the Academy network
- Mobile phones (personal or otherwise) connected to the Academy Wi-Fi
- I-pads
- Android tablet devices
- Cameras or other portable storage devices.

## Security Advice and Guidance

**Avoid theft - Equipment**

To avoid theft, lock classroom doors when not in use and/or place devices in secure areas when not in use.

**Care when transporting equipment or data**

Take care when transporting or storing devices outside the Academy. Devices are not covered by the Academy insurance policy if lost, stolen or damaged off-site. Care should be taken when transporting devices in bags with liquid. USB devices should be encrypted for advice please see the ICT Network Manager at your Academy.

**Protecting your identity**

In order to protect your identity and data:

- Never allow anyone else (especially students) to use your laptop or device
- Never give your password to anyone. Divulging your password to a student enables them to access areas of the network which are sensitive
- Change your passwords regularly
- Never give your details to an unknown source via email
- Do not post pictures or information about yourself on public websites (accessible to students or parents). Restrict access!

**Data Security**

Never leave yourself logged onto the network or leave devices unattended. Encrypt your data if sending via email or save to a secure folder.

Protection of data is the responsibility of the end user. In particular:

- Never lend your device to someone else (staff, family member or student)
- Do not give out your password to anyone
- Ensure your password is secure
- Change your password regularly
- Do not leave devices unattended with data on the screen
- Password protect your information
- Do not store sensitive or personal information in public areas or cloud based storage
- Do not store sensitive information on portable USBs (unless encrypted).

Users need to be aware that sensitive data is not confined to SIMS. It could include any material kept on the VLE/ Doddle that identifies data subjects. What is meant by sensitive data? This includes:

- Data held in SIMS (names, addresses and personal details)
- SISRA or similar
- SEND register
- Information of a personal nature.

**Good Practice Backing-Up**

Technology lets us down from time to time. Therefore it is recommended that you:

- Save your work to your user area (this is backed up)
- Save work regularly
- Always make more than one copy
- Save work to the network (in secured areas only).

**Storage Security Cloud Based Technology**

Please note that work saved to cloud based technologies is not covered or protected by the Academy or backed up. Data stored here is potentially vulnerable and done so at the owner's risk. Sensitive data must never be stored in this way.

**Monitoring Inappropriate Activity**

Please note that the Academy does have the ability to monitor activity on the network. If inappropriate use is reported or suspected then usage can be traced back to source or monitored and action may be taken.

**Software**

You should rarely need to add software yourself. For devices issued by the Academy:

- All devices are configured for general use
- No software should be installed without ownership of the licence (in the case of an I-Pad the user may own the licence)
- Inappropriate images, videos or games must not be downloaded or stored on devices
- Do not download files from unknown sources

*If in doubt, ask.*

**Virus Protection**

- Laptops are installed with anti-virus software. However, they need to be connected to the network in order to update the software and check for threats. Please connect regularly.
  *If you have a problem, please contact the ICT team.*

**Avoiding Viruses**

Good practice to avoid viruses includes:

- Caution when downloading software
- Caution when opening email attachments from senders with whom you are not familiar. All such emails should be deleted upon receipt.

**General**

The following points follow a set of general principles when connecting devices (Academy owned or personal) to the Academy network, Wi-Fi. The same rules apply to home.

When using devices issued by the Academy or when connected to the Academy Wi-Fi employees must not:

- Use the device in pursuit of any activity that is illegal
- Download or otherwise make use of pornographic, excessively violent or other inappropriate images or films of any kind
- Engage in sending or receiving images of students
- Engage in forms of communication (either in or outside of school) with students that could be construed as being or likely to be in *contravention of child protection guidance*. This includes:
    - Facebook*
    - Twitter*
    - Whatsapp*
    - Snapchat*
- Other similar on-line community websites.

Please note, some subject areas do use Twitter accounts specifically set up to share ideas and subject content with students. Please note that these accounts are not subject to filtering. Staff should therefore monitor postings and content of these accounts carefully. As a rule, it is recommended that all communication with students is conducted through Academy email accounts or the Virtual Learning Environment (VLE/ Doddle). Please take advice from Lisa Plowman before engaging in other forms of electronic communication.

**Personal Use of Social Media Sites**

All employees should take care when using Facebook and other social networking sites. This includes:

- Ensuring that their postings do not bring either them or the Academy into disrepute
- Not sharing personal information about other employees on public forums or social media.

Remember, content and personal details may be viewed by students or parents. This includes: photos or other sensitive information. As such, be careful what is posted.

Staff should not use Facebook or other Social Media sites during their dedicated working hours.

**Reporting Misuse or E-Safety Concerns**

Academy staff are requested to **report suspected inappropriate use of technology** by either students or other Academy employees to:

- Lisa Plowman, Vice Principal

Your concern will then be directed to the appropriate person (Child Protection, Bullying etc.).

**For all other issues** (technical) please report using the Academy **reporting on-line system to**:

- Ian Hopkins – Partnership ICT Manager
- Dom Saunders – Ernulf

***The on-line booking system can be found on the intranet/staff link.***

**Acceptable Use: Email and Social Networking**

Staff should only use their Academy email account for Academy business. This includes:

- Student progress
- Department business
- Student support issues
- Whole-Partnership issues
- Emailing parents (assertive mentoring/tutors/class teachers)
- Communication with feeder schools or other secondary colleagues
- Businesses or other agencies directly relating to Academy events or activities
- Clubs and activities.

Staff should not send generic emails to **whole year groups** or to the **whole-staff** without prior agreement with a senior member of staff.

**Communication to parents of whole year groups or whole-staff**

If there is a need to communicate to whole year groups, first liaise with your HOD and SLT link. These communications are kept to a minimum otherwise they lose their impact.

**Mobile Phones**

Staff should use personal mobile devices responsibly. For your protection:

- Staff should not contact students using personal mobile phone (this includes texting)
- If on trips or visits, staff should use one of the Academy mobile devices which are available through resources
- Staff should never divulge personal mobiles numbers or information to parents or students.

**Personal Calls** - *Mobile phones should not be used to take personal calls in the classroom or in the corridors.* All staff are contactable in an emergency via Reception.

**VLE**

The VLE is accessible to both students, parents/guardians and staff. As such staff should check which folders are accessible to students and/or other staff before storing information here.

Staff should ensure that:

- Care is taken about storing sensitive information on the VLE
- Care is taken to ensure that inappropriate web links are not posted or made available
- If using Forums, Surveys or Wiki facilities, it is the responsibility of the classroom teacher to monitor the sensitivity, appropriateness and on-going language used. Anything inappropriate must be removed and reported to the ICT network manager or member of SLT.

**Photographs and Video**

If, as part of a lesson, trip or activity video or photographs are taken, staff should:

- Transfer the video or photograph to the server as soon as possible and delete from the device to avoid someone else accessing the images
- Ensure that the video or photographs are wholly appropriate
- Check with a member of SLT if you are intending to publish any images (there is a list of those students whose parents have prohibited the use of their child's image. The member of SLT will check whether permission to use the image is allowed (A list of students whose image may not be used is displayed in the Admin office and the PA to the Principal's office)

In addition, staff should avoid storing personal photographs or video on Academy devices in case they fall into the hands of students.

**E-Safety & Students**

If you are using technology as part of a lesson it is **your responsibility to monitor** the activities of students in your charge. This includes:

- Safe use of the internet
- Appropriate use of technology (cameras, video equipment)
- Misuse and damage (and reporting this).

Teachers or other persons supervising young people should monitor use of technological equipment and report any misuse such as:

- Downloading or accessing inappropriate materials
- Sending or receiving indecent images (on any device)
- Sending or receiving malicious emails or texts
- Wilful damage of equipment
- Cyber bullying
- Other issues of e-safety.

**Use of Mobiles by Students BYOD "Bring Your Own Device"**

We intend to roll out BYOD across the Academy. Students will be asked to sign up to an acceptable use agreement as part of the provision. Wi-Fi hotspots will be made available. Full Wi-Fi coverage is not possible. Students using BYOD can access the internet (on a secure filtered separate network).

As a rule students are not allowed to use their mobile devices on school site. However, some teachers may wish to include smart phones as part of a learning activity and take advantage of Bring Your Own Device (BYOD).

If considering using personal devices (belonging to students) as part of a lesson please think carefully about:

- How the activities are going to be monitored (accessing the internet, sending or receiving texts or images)
- What will happen to the data afterwards?
- Wow will you ensure that students are on task?
- How will you ensure that students are using their devices appropriately?
- What happens if a device is damaged or goes missing?

*Remember, planning is key!*

**Care of Equipment**

If employees use an ICT room and the equipment is not fully functioning, please report this to the ICT Network Manager. Do not leave it to the next person.

**Summary**

Key points to remember:

- Take security seriously
- Watch your e-footprint
- Never divulge your password to students or other staff except to authorised personnel such as the ICT Team
- Use only pre-installed software or that for which you have a licence
- No inappropriate material or downloads
- Back up your work
- Think 'child protection', 'data protection' and general safeguarding
- Always keep a back-up.