Supreme Education

'to educate and inspire through SUPREME learning'

Acceptable Use Policy

Reviewed: December 2020

Supreme Education Acceptable Use Policy

DEFINITION

Information and Communication Technology (ICT) includes computers, mobile phones, iPods, tablets, cameras, microphones, flash drives and any other electronic means of storing, communicating or processing graphical, textual or audio information.

RESPONSIBILITIES OF ALL USERS

- All users must be active participants in e-safety education, taking personal responsibility for their awareness of the opportunities and risks posed by new technologies.
- All users have a responsibility to report any known misuses of technology, including the unacceptable behaviours of others.
- All users have a duty to respect the technical safeguards which are in place. Any attempt to breach technical safeguards, conceal network identities, or gain unauthorised access to systems and services, is unacceptable.
- All users have a duty to report failings in technical safeguards which may become apparent when using the systems and services.
- All users have a duty to protect their passwords and personal network logins, and should log off the network when leaving workstations unattended. Any attempts to access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.
- All users should use network resources responsibly. Wasting staff effort or networked resources, or using the resources in such a way so as to diminish the service for other network users, is unacceptable.
- All users should understand that network activity and online communications are monitored, including any personal and private communications made via the centre network.
- Students are allowed to use electronic devices such as smartphones, Tablets and MP3 players, during break or lunch time. However they must be turned off and put away during lesson time.

When an electronic device is brought into the centre, it is entirely at the students own risk. The centre accepts no responsibility for the loss, theft or damage of any electronic device brought into the centre.

- If a member of staff has asked a student to put the device away three times and the student still refuses to comply, then after the third request the item can be confiscated and given to the admin office.

- All property confiscated by staff is to be given to the main reception. Items may be collected at the end of the day, however, for repeated offenses, parents will be asked to come in and collect the item.

- The “Supreme Education acceptable use policy” applies to the use of all technology in the centre or during an activity organised by the centre on or off site.

- Student’s must not attempt to access material that is unsuitable or attempt to misuse centre networks and facilities

- No digital pictures or footage should be taken of any member of the centre community without their permission. If a member of staff catches anyone doing this, they should in the first instance report this to SLT this is because some maybe useful as evidence

- Any footage uploaded onto a social media network showing the centre in bad light, or bringing the name of the centre into disrepute will be deemed a very serious offence. The person in question will therefore risk disciplinary sanctions being taken against them.
- All users must take responsibility for reading and upholding the standards laid out in the AUP.
- All users should understand that the AUP is regularly reviewed and consistently enforced.

E-SAFETY
All members of staff are responsible for protecting students from the following sources of possible risk arising from the use of ICT:

	Commercial	**Aggressive**	**Sexual**	**Values**
Content (Child as recipient)	Adverts, Spam, sponsorship, Personal info.	Violent/hateful content	Pornographic or unwelcome sexual content	Biased, racist, misleading info. or advice
Contact (Child as participant)	Tracking and harvesting personal info.	Being bullied, harassed or stalked	Meeting strangers, being groomed	Self-harm, unwelcome persuasions
Conduct (Child as actor)	Illegal downloading, hacking, gambling, financial scams, terrorism	Bullying or harassing another	Creating and uploading inappropriate material	Providing misleading info/advice

Controlling access is a necessary part of e-safety in the centre, but the overall approach we adopt is to equip students with the skills and knowledge they need to use technology safely and responsibly, and manage the risks wherever and whenever they go online.

Responsibilities of **all members of staff** include:

- Supervising students’ use of ICT in lessons and at all other times.
- Controlling and monitoring students’ access to and use of ICT.
- Reporting any abuses of ICT in the first instance to the ICT Co-ordinator and if necessary passed onto the Safer centres Officer or the head of centre.
- Supporting students in becoming safe users of ICT, in particular by reinforcing e-safety through the ***SMART*** rules.
- Maintaining appropriate professional distance in communicating with all students attending the centre, by not allowing current students as personal contacts on social networking sites, and never to post images of or comments about students on the Internet.
- To support the centre’s policy for recording and using students’ images, by reading Appendix A of this document and checking pupils’ permission status on the Staff Shared Area.
- To use only the centre’s email system to communicate with students and not to share personal email addresses with them.
- To use the centres telephone system to communicate with students and not to share personal telephone numbers with them.

Responsibilities of **Teachers** include:

- Familiarising themselves with basic e-safety issues and the ***SMART*** rules in particular by using the ***“Know it all”*** resources on the centre’s network and by seeking advice from the ICT Co-ordinator where necessary.
- Displaying the ***SMART*** rules by the classroom computers.
- Using ***Impero Console (IC)*** to manage students’ use of computers, taking care:
    - Never to allow students to use the ***IC*** program.
    - To keep the ***IC*** program on the task bar while it is running.
    - To always freeze or blank the ***IWB*** when operating the ***IC*** program.
    - To always lock the teacher’s computer when it is not in use, even if members of staff are present in the room.
    - Never to allow students to use the teacher’s computer unless they have one-to-one supervision.
    - To take all precautions to protect staff passwords and the wireless network password.

Responsibilities of the **ICT Co-ordinator** include:

- Ensuring that all students have been introduced to the ***SMART*** rules.
- Supporting staff and students in becoming safe ICT users.
- Supporting staff in using the centre's network.
- Monitoring the safe use of the centre's network.
- Informing the Head Teacher and Safer centres Officer of any safety issues that arise and working with them to resolve them.
- Providing or organising the training of staff where needed.
- To work with staff in reviewing and revising this policy once a year.
- To advise parents and carers on supporting e-safety with their children.

ACCEPTABLE COMPUTER USE

The centre's computers are provided primarily to support students' learning and members of staff are expected to help students to accept this, and to support each other by maintaining a consistent approach across the centre. In particular:

- Not to bargain work or good behaviour for ***"free time"*** on the computer, where free time is: listening to music, playing games, using a social networking site, watching videos on YouTube or emailing etc
- Not to use ***"free time"*** as a means of pacifying a student or occupying them when they have refused other activities or are not catered for.
- To encourage pupils to expect that ***"free time"*** is acceptable only during break and lunch times as a leisure activity.
- Not to allow students to listen to music while they are doing their work on the computer.
- To develop a set of clear expectations and routines for the use of computers in each subject area.

CARE OF COMPUTERS

Students need to be encouraged to respect the ICT equipment and the opportunities it offers them. At Supreme Education students often target the ICT equipment when they are emotional or attempting to manipulate staff. Experience has shown that the following points are helpful to remember:

- Staff and student safety is always the first priority no matter how expensive the equipment.

- Avoid over reacting to the equipment being targeted by students as this inevitably leads to an escalation of the damage; try the same level of reaction as for a pencil or a book.
- Avoid wrestling the equipment from students as this inevitably leads to more damage.
- Holding the equipment or placing yourself or your hands between it and the student will often calm things down; out of site and out of mind.
- Divert the student's attention away from the damage being done and towards his behaviour.
- Provide clear choices and consequences for the student's behaviour, where the focus is respecting the equipment and not the damage.
- Discuss consequences for the damage done after the event, when things are calmer.

Members of staff are expected to model and guide students in good practice in the use of computers, for example:

- Logging off each session.
- Saving work at regular intervals and with useful titles in organised folders.
- Maintaining the work stations in each room with monitor, keyboard, mouse and chair in the same position and encourage the students to leave it in the same way. Pupils are more likely to leave the equipment tidy if they find it tidy.
- Keep the monitors, keyboards and mice free from smears and grim by cleaning them regularly using the cloths and fluids provided.
- Taking action to remove any graffiti from equipment, including benches, and reporting this and any other damage to the ICT co-ordinator.

MONITORING

The centre's network is monitored by ***Impero Console*** software. This allows users computer activity to be logged and evidence to be collected once unacceptable use has been identified. Examples of unacceptable use will be reported to the Head teacher and he, together with the Safer centres Officer, will pursue these and decide on the degree of escalation and action to be taken, including sanctions.

APPENDIX A

Use of Pupil Images Policy

All pupils must have a "**Supreme Education centre Use of Image Consent Form**" completed by parents/guardians before images are recorded.

Staff must check the student's permission status on the Staff Shared Area of the centre's network if they are recording or using images of students.

Parents are informed of the following guidelines that we maintain:

1. We may use photographs or recordings after your child leaves the centre, until the event or issue they depict is no longer current.

2. We will not use the personal details or full names (which means first name and surname) of any child or adult in a photographic image on video, on our website, in our centre prospectus or in any of our other printed publications.

3. We will not include personal email or postal addresses, or telephone or fax numbers on video, on our website, in our centre prospectus or in other printed publications.

4. If we use photographs of individual pupils, we will not use the name of that child in the accompanying text or photo caption.

5. If we name a pupil in the text, we will not use a photograph of that child to accompany the article.

6. We may include pictures of pupils and teachers that have been drawn by the pupils.

7. We may use group or class photographs or footage with very general labels, such as "a science lesson" or "making Christmas decorations".

8. We will only use images of pupils who are suitably dressed, to reduce the risk of such images being used inappropriately.