



Dream Believe Achieve

ICT Policy

Signed by Chair of Governors

Kerry Scott

Date ratified by Governors

07/12/2022

Date to be reviewed by Governors

07/12/2023

Belmont Park School Policy and Protocols

For Students use of Information and Communication Technology

Including the Internet and email

Student Computer User Agreement

Students are encouraged to use the schools ICT facilities to support their learning however we ask that all students respect the school's ICT equipment and facilities. By logging on to the school computer network and/or using the schools ICT equipment, students agree to the contents of this policy. We ask parents to support us in this matter. Students are asked to sign a copy of the Use of ICT. Frontier and Internet agreement in their School Journals (Appendix A).

Expectations for using the school's ICT equipment.

Students should:

- Use ICT to support, enhance and extend their learning.
- Be efficient in their use of resources.
- Avoid waste (Including paper, ink and electricity) – where possible print on both sides of the page.
- Recycle used paper.
- Only use the school's ICT equipment when given permission to do so by a member of staff.
- Only use ICT equipment and the wireless network for school approved activities.
- Keep passwords secret and never knowingly let another student access their user area.
- Use suitable file names and keep their user area organised so that they can easily find their work.

Students should:

- Not misuse, vandalise or damage any item of ICT equipment.
- Not send messages or produce documents containing bad language or anything which is likely to offend others.
- Not send offensive or threatening material or comments to or about members of the school community or others using computers, mobile phones or other devices from inside or outside the school.
- Not intentionally seek out rude sexually explicit, offensive, violent, hateful discriminatory material on the internet.
- Inform a member of staff if they accidentally come across something on the internet or in an email that a reasonable person would consider to be rude sexually explicit, offensive, violent hateful discriminatory or likely to bring the school into disrepute.

- Not attempt to hack or bypass the school's security and filtering systems.
- Not run or attempt to run executable files brought in on a USB
- Not breach copyright eg. by copying information from the internet or somebody else and presenting it as their own work.
- Never tamper with or attempt to fix terms of school equipment eg. they should not attempt to clear paper jams, move equipment, disconnect or reconnect cable, refill paper trays, change printer cartridges, change batteries etc.
- Understand that members of staff have access to Internet, Keyword & Phrase and software application monitoring software. Monitoring software will be used to support our students with E-safety and enhance our safeguarding policy. Members of staff also have access to students are not breaking school rules.
- Report any malfunctioning or damaged equipment or software to a member of staff.
- Understand that refusal to follow the school's expectation may result in a punishment.

Unless given permission by a member of staff as part of a learning activity or approved application process, students should:

- Not visit chat rooms, social networking, games or entertainment sites.
- Not give not their full name, home address, telephones numbers, personal or school email address over the internet or in emails.
- Never send personal photographs and images of themselves or others over the internet or in email.
- Never arrange to meet somebody over the internet or vial email.
- Not download or upload material files.

User ICT equipment outside the classroom

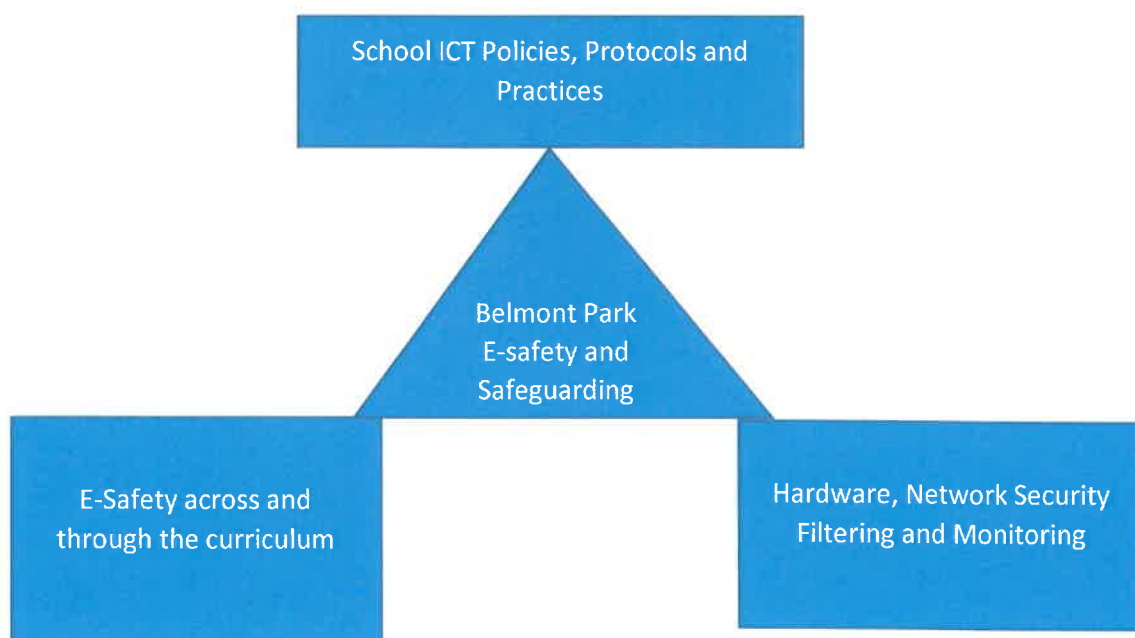
There may be occasions when students are allowed to use ICT equipment outside of the classroom eg. laptops, notebook computers, netbooks, PDAs, cameras, recording devices, data logging equipment etc.

When using ICT equipment of the classroom students should:

- Make sure that they have gained permission from a member of staff and signed any relevant forms.
- Make sure that a member of staff knows where they will be working.
- Take care that of the equipment and where practicable, keep it out of sight of others, particularly if they have been given permission to take the equipment off-site.
- Inform their parents that they have school equipment at home.
- Keep the equipment in a safe place.
- Observe instructions about returning the equipment.
- Report any malfunctioning or damaged equipment to a member of staff and return the equipment as instructed.
- Not intentionally introduce any viruses or non-approved software on to the device.

This ICT policy should be considered in conjunction with Belmont Park School's other policies, procedures and protocols designed to promote the safeguarding of students.

The use of Technology in education has and will continue to develop at a rapid pace. Like other schools, Belmont Park school expects, encourages and promotes the use of ICT as a tool to promote, support and extend learning opportunities for our students. However, the growth in the use of ICT gives the rise to additional dangers that students, staff and parents need to be aware of and take precautions to guard against.



Policies, protocols and practices

These are codified ways of working that clearly set out expectations governing the use of ICT equipment in the school and date about individual members of the school community. These policies, protocols and practices are designed to reduce the risks and dangers that arise from the increasing use of Information and Communications Technology in the school.

Hardware and network security

Belmont Park School ICT support Department ensures that its computer network is safe, reliable and set up and maintained in such a way to minimise the risks inherent in the use of ICT equipment, the most common of which arise from young people accessing unsuitable material online.

E-safety across and through the curriculum

Students at our school have to be taught how to stay safe when using ICT equipment both at school, at home or in the community. Staff understand that it is not just the job of the ICT curriculum to teach e-safety training must be taught across the curriculum.

Laws and regulations governing the use of computers

Students and parents need to be aware of the following laws and regulations governing the use of computers, either at school, at home or in any other location:

- The Copyright Design and Patents Act (1989)
- The Computer Misuse Act (1990)
- The Data Protection Act (1984)
- The Digital Economy Bill (2010)
- The Communications Act 2003 (Section 127)
- The Communications (Television Regulations) (2004)
- The Freedom of Information Act (2000)

The Copyright, Design and Patents Act

The law prohibits the copying of computer file without permission from the owner or the copyright holder. This law makes it illegal to:

Use of software without a proper licence.

Download and use text or images from the internet without permission from the copyright owner or without acknowledging the source.

Copy a computer program to run on another computer without permission from the copyright holder.

The Computer Misuse Act

This law makes it illegal to:

Attempt to gain unauthorised access to computer material or parts of a computer network (hacking) that you are not permitted to see and it outlaws the illegal copying of computer programs (commonly known as software piracy).

Gain unauthorised access to a computer to carry out a crime.

Change computer files with authorisation, including planting viruses and deleting files.

The Data Protection Act

This law gives rights to anybody who has data about them stored on a computer. The Act has eight principles. The eight principles of the Data Protection Act are that:

- 1) Data must not be processed unless there is a specific lawful reason to do so.
- 2) Data must only be obtained and then used for specific lawful reason to do so.

- 3) Data should be adequate, relevant and not excessive for the specified use.
- 4) Data must be accurate and, where relevant kept up to date.
- 5) Data should not be kept longer than necessary for the specified purpose.
- 6) Data should meet the legal rights of the data subjects.
- 7) Data holders should protect the data against loss, theft or corruption.
- 8) Data should not be transferred abroad, except to certain European countries.

The Digital Economy Bill

This legislation was passed at the end of the last Parliament. It allows persistent illegal file shares to be disconnected from the Internet. This means that your Internet service could be suspended or removed if you or anybody else in your household repeatedly, illegally downloads files from the Internet, including copies of computer games and music files. This piece of legislation will be scrutinised (looked at) by the new Government before it becomes law.

The Communication Act 2003 (Section 127)

Anyone sending by means of the Internet, a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of, or persistently making use of the internet for the purposes of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction to imprisonment. This law means that an offence is committed as soon as the message is sent there is no need to prove any intent or purpose.

The Communication (Television Licensing) Regulations (2004)

Parents and students should know that they need to be covered by a valid TV licence if they watch or record TV as it is being broadcast. This includes the use of devices such as a computers, laptops, mobile phones or DVD/video recorders. As new technology makes it possible to watch TV on more devices than ever parents need to make sure that their family remains properly licensed. If you or your children watch or record television programmes they are being shown on TV you must, by law be covered by a TV licence, no matter what device you are using. Outside of school, students will be covered by their parents TV licence at the address where they live.

Computers and Laptops

Many TV channels are now available to watch over the internet. If students are watching programmes on a computer or laptop as they are being shown on TV, then they need to be covered by a TV licence. However, people do not need to be covered by a licence if they are only using 'on demand' services to watch programmes after they have been shown on TV. So, you need to licence to watch any channel live online, but you wouldn't need one to use services such as BBC iPlayer or 4oD to catch up on episode of a programme you have missed.

Mobile phones

Just as with any other device, if students are watching programmes as they are being shown on TV on a phone or any other mobile device, they need to be covered by a TV licence. If a student is covered by their parents' valid licence at the address where they live, they will be licensed to use any device powered solely by its own internal batteries outside of their home too.

Virgin, Sky+ games consoles and digital TV recorders

If students use Virgin+, Sky +, Playstation or any other games console or a digital TV recorder to watch or record programmes as they are being shown on TV, they need to be covered by a TV licence. This is also the case if they use a DVD/VHS recorder. If they only use a digital box to produce sounds (ie. It is never used to display television programmes) then they do not need to be covered by a TV licence.

The Freedom of Information Act (2000)

The Freedom of Information Act gives parents and students the right to ask for all of the information any public organisation, including schools, has, including any personal information the organisation holds about their child/you. Public bodies (including schools) can withhold certain information for example, they would not give out personal information about somebody else's child, or pre-release information before a publication date e.g exam results. For further advice or your rights visit direct.gov.uk and type Freedom of Information into the search bar.

Appendix A

Use of ICT and the Internet

We expect and encourage students to use the school's ICT facilities and the internet to support and enhance their learning. Before your child is allowed to use our ICT equipment and the internet we expect all parents and students to read and sign and this agreement. A copy of the Belmont Park Computer User Agreement Policy can be found on our website.

Students must:

- Only use the School's ICT equipment and the Internet when given permission to do so by a member of staff.
- Not disclose their home address/telephone number or any other personal details that could be used to trace them unless permission has been given by parents and a teacher.
- Not send personal photos of themselves or others over the internet without permission of parents and a teacher.
- Never use the Internet or email to arrange to meet anybody in person unless permission has been given by parents and a teacher.
- Not use bad language in their email messages.
- Not send offensive or threatening material or comments to anyone – including to or about members of the school community or others – using computers, mobile phones or other devices from inside or outside of school.
- Not intentionally seek out offensive materials (eg. distasteful, hateful rude or violent text or images).
- Inform a member of staff immediately if anything offensive, dangerous, likely to be harmful to or cause upset others, or anything that is likely to bring the school into disrepute appears when they are online.
- Understand that staff have access to internet, Keyword and Phrase and software application monitoring software. Monitoring software will be used to support our students with E-safety and enhance our safeguarding policy. Members of staff also have access to students' user areas, email messages and other internet related files and that these are monitored to ensure expectations of behaviour are being met.
- Understand that refusal to comply with these expectations may result to ICT equipment or the internet being denied.

Unauthorised use and/or damage to ICT equipment or unauthorised use of internet facilities or attempting to/or visiting inappropriate websites and social networking sites or with the wilful introduction of viruses to the school network will result in punishment.

As a user of the school's ICT equipment and the Internet, I agree to comply with the expectations set out above and in the Belmont Park School Computer User Agreement Policy.

Signed Student: _____ Date: _____

Parental Agreement

I understand the students will be held accountable for their own actions. I also understand that some materials on the Internet may be objectionable and I accept responsibility together with the school, for the explaining to my child the expectations they are supposed to follow when using computers, the internet and email.

Signed Parent: _____ Date: _____

Name of Parent: _____