Education 1st
"enhancing lives through education"
Sports 1st

07341 564 377
admin@education-1st.org.uk
www.education-1st.org.uk

ICT Acceptable Use Policy

Policy Review
The responsibility of reviewing and maintaining this policy is Craig Dembicki (Managing Director). This policy will be reviewed annually.

Start date of policy: **1st June 2015**
Last review date: **2nd August 2021**
Date of next review: **1st August 2022**

Signed Date: 2nd August 2021

Craig Dembicki
Managing Director
Education 1st

Purpose

The purpose of this policy is to lay down clear expectations for the safe and purposeful use of the provisions' ICT resources. It aims to highlight good practice that engages students, facilitates and enriches teaching and learning and upholds Education 1st's duty to safeguard its students and employees. It also recognises the role that parents and carers play in using ICT at home and can be used to support online learning or leisure activities in a supportive manner outside the provision context.

New technologies form an essential part of young people's lives, both in provision and at home. We believe it is our duty to prepare students for life in the 21st Century through educating them about the safe and effective use of such technologies and providing opportunities for them to explore the digital world in a safe environment.

This policy also lays out expectations for staff and students when using ICT outside the education environment particularly when using the provisions equipment (i.e. a staff tablet). Of particular note for staff is the guidance on social networking. All users are expected to act responsibly and to show consideration to others.

Technology that can be used to store, transmit or manipulate data, such as smartphones and tablets should be used responsibly and in accordance with the ICT Acceptable Use Policy, even when not used with the provisions' equipment.

Related Policies

- Anti-Bullying Policy
- Attitude to Learning (Behaviour) Policy
- Child Protection and Safeguarding policy
- Confidentiality Policy
- E-safety Policy
- Data Protection Policy
- Device, Google Drive and BYOD Policy

Responsibilities:

Users are responsible for the protection of their own account and must, therefore, keep passwords confidential. Passwords must be complex: a minimum of 6 characters, which are advised to include uppercase and lowercase letters and numbers. Users may only log on to their own account and must log off when leaving a workstation, even for just a short period of time.

It is not acceptable to:

- Attempt to download, store or install software to the provisions' computers /ipads/tablets
- Attempt to introduce a virus or malicious code to the network
- Attempt to bypass network or system security
- Attempt to access another user's account
- Attempt to gain access to an unauthorised area or system
- Attempt to use any form of hacking/cracking software or system
- Connect any device to the network that acts as a Wireless Access Point (WAP), bridge or router
- Physically damage or vandalise any computer equipment
- Access, download, create, store or transmit material that; is indecent or obscene, could cause annoyance or offence or anxiety to others, infringes copyright or is unlawful, brings the name

Education 1st into disrepute (e.g. using the internet at the centre to download files, materials or applications that could be considered racially or sexually offensive)

- Engage in activities that waste technical support time and resources.

Privacy and E-Safety

Users should realise that the provision has a right to access personal areas on the network. Students are expected to act safely by not publishing online personal information. They may share interests, ideas, and preferences. Students must not give out their family name, password, username, email address, home address, provision name, city, county or other information that could help someone contact or locate them in person. It is not acceptable to engage in any behaviour that is upsetting or threatening to another user. Even friendly or flattering comments may be construed as upsetting if they are unsolicited or unwanted. Any form of online bullying will be dealt with in line with Education 1st's Anti-Bullying Policy
Users should not forward private data without permission from the author.

Internet Access

The use of public chat facilities is not permitted unless directed by a teacher as part of online learning. Users should not attempt to use proxy servers to bypass the internet filter system. Users should not copy and use material from the Internet to gain an unfair advantage in their studies, for example in coursework. Such actions may lead to disqualification by examination boards. Information sources should be referenced. Users should ensure that they are not breaking copyright restrictions when copying and using material from the Internet. Users should not attempt to access or create material that is unlawful, obscene or abusive.

Email

Students are not allowed to use email during lessons, unless the teacher for that lesson has permitted its use. If a user receives an email from an unknown person or that is offensive or upsetting, a senior member of staff should be contacted. They should not delete the email in question until the matter has been investigated .Sending or forwarding chain emails is not acceptable. Users should not open attachments from senders they do not recognise, or that look suspicious. Users should periodically delete unwanted sent and received e-mails.
Staff sending sensitive information via email should use best practice to ensure that information is sent to the intended recipient in a secure manner.

Blogs

Language that is not appropriate for class is not appropriate for a blog. Users are expected to conduct themselves as representatives and ambassadors of the provision. They must not post comments that are defamatory about the provision, staff or students or messages which may cause offence or be upsetting. If a user receives a message from an unknown person, or which is offensive or upsetting, an appropriate staff member should be contacted (e.g.
Operations Manager) Users must respect other users' work and opinions and not maliciously edit any group or individual work. Any user who feels this has taken place should leave the work as it is and contact a relevant member of staff.

Social Networking

For the purpose of this policy, social media is the term commonly used for websites which allow people to interact with each other in some way – by sharing information, opinions, knowledge and interests. Social networking websites such as Facebook and Twitter are perhaps the most

well-known examples of social media but the term also covers other web based services such as blogs, video and audio podcasts, message boards, photo document and video sharing websites such as YouTube. This definition of social media is not exhaustive as technology develops with new ways of communicating advancing every day.
For the purpose of this document the terminology Social Media is not exhaustive and also applies to the use of communication technologies such as mobile phones, cameras or other handheld devices and any other emerging forms of communications technologies.

Education 1st Social Networking (SN) expectations for students:

Students are not allowed to use SN facilities during lessons, unless the teacher for that lesson has permitted its use and it complies with Education 1st" Devices Policy.
If a user receives a message from an unknown person, or which is offensive or upsetting, an appropriate staff member should be contacted. Users should perform a 'print screen' and paste the message into MS Word, noting the date and time and saving the document until the matter has been investigated. Users should only communicate with people on their contact or buddy list.
Students should not accept requests to join their contact list from people not already known.
Students should never accept files or downloads from people not known, or that look suspicious.
They should not use a screen-name that is offensive, or gives away personal information. They should not add or allow their profile, screen-name or contact information to be shown in online public directories.
Users should not upload images of themselves or others that could be considered inappropriate or damaging. They should not write messages about others that could be misunderstood or misinterpreted.

Education 1st's Social Networking expectations for all staff including volunteers:

All adults working with students have a responsibility to maintain public confidence in their ability to safeguard the welfare and best interests of students. It is therefore expected that they will adopt high standards of personal conduct in order to maintain the confidence and respect of their colleagues, students, public in general and all those with whom they work in line with the provision's code of conduct. Adults in contact with students should, therefore, understand and be aware that safe practice also involves using judgement and integrity about behaviours in places other than the work setting.
The guidance contained in this policy is an attempt to identify what behaviours are expected of adults within the provision setting who work with or have contact with students. Anyone whose practice deviates from this document and/or their professional or employment related code of conduct may bring into question their suitability to work with children and young people and may result in disciplinary action being taken against them.
Adults within the provision setting should always maintain appropriate professional boundaries and avoid behaviour, during their use of the internet and other communication technologies, which might be misinterpreted by others. They should report and record any incident with this potential.
In their own interests, adults within provision settings need to be aware of the dangers of putting personal information onto social networking sites, such as addresses, home and mobile phone numbers. This will avoid the potential for students or their families or friends having access to staff outside of the provision environment. It also reduces the potential for identity theft by third parties.
All adults, particularly those new to the provision setting, should review their social networking sites when they join Education 1st to ensure that information available publicly about them is accurate and appropriate. This includes any photographs that may cause embarrassment to themselves and the provision if they are published outside of the site

Adults should never make a 'friend' of a student at Education 1st where they are working on their social networking page or become 'friends' with ex-students, parents or carers. If a member of staff feels they have exceptional circumstances to deviate from this guidance, this needs to be agreed with the Designated Safeguarding Lead.
Staff should never use or access social networking pages of students and should never accept an invitation or invite a student to become a 'friend'.

Confidentiality needs to be considered at all times. Social networking sites have the potential to discuss inappropriate information and employees need to ensure that they do not put any confidential information or images on their site about themselves, their employer, their colleagues, students or members of the public
Employees need to ensure that when they are communicating about others, even outside of work, that they give due regard to the potential for defamation of character. Making allegations on social networking sites (even in their own time and in their own homes) about other employees, students or other individuals connected with the provision, could result in formal action being taken against them.
Adults are also reminded that they must comply with the requirements of equalities legislation in their online communications
Adults within the provision setting must never post derogatory remarks or offensive comments online or engage in online activities which may bring Education 1st into disrepute or could reflect negatively on their professionalism.
Some social networking sites and other web-based sites have fields in the user profile for job title etc. Staff are strongly advised to remove their place of work from social media sites to avoid potential conflict.

Protection of personal information:
Adults working in Education 1st should:

- Never share their work log-ins or passwords with other people
- Not give their personal email addresses or information to students or parents.
- Where there is a need for information to be sent electronically, the provision email address should be used
- Keep their phone secure at all times
- Not use ICT equipment for personal use, unless it has been authorised and appropriate insurance has been obtained (e.g. camera or recording equipment)

.

Communication between students / adults working in provision
Communication between students and adults by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones, text messaging, emails, digital cameras, videos, web-cams, websites and blogs.

Adults should not request, or respond to, any personal information from a student or parent/carer, other than that which might be appropriate as part of their professional role. Adults should ensure that all communications are transparent and open to scrutiny. They should also be circumspect in their communications with students so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as 'grooming' in the context of sexual offending.
E-mail or text communications between an adult and a student outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications through internet based websites. Internal email systems should only be used in accordance with the Education 1st

policy. Staff should use blocking procedures for nuisance callers and should report this to their line manager.

Access to inappropriate images and internet usage:

There are no circumstances that will justify adults possessing indecent images of children. Staff who access and possess links to such websites will be viewed as a significant and potential threat to children. Accessing, making and storing indecent images of children is illegal. This will lead to criminal investigation and disciplinary action being taken

Adults should not use equipment belonging to their provision/service to access any pornography; neither should personal equipment containing these images or links to them be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with children.

Adults should ensure that students are not exposed to any inappropriate images or web links. Where indecent images of children are found, the police, local authority designated officer (LADO) and provision Designated Safeguarding Lead will be immediately informed. Colleagues should not attempt to investigate the matter or evaluate the material themselves, as this may lead to evidence being contaminated which in itself can lead to a criminal prosecution. Where other unsuitable material is found, which may not be illegal but which raises concerns about that member of staff the LADO should be informed and advice sought. Colleagues should not attempt to investigate or evaluate the material themselves until such advice is received.

Cyber-bullying

Cyber-bullying can be defined as 'the use of modern communication technologies to embarrass, humiliate, threaten or intimidate an individual in an attempt to gain power and control over them.' Prevention activities are key to ensuring that adults are protected from the potential threat of cyber-bullying. All adults are reminded of the need to protect themselves from the potential threat of cyber-bullying.

If cyber-bullying does take place, employees should keep records of the abuse, text, emails, websites or instant message and should not delete texts or emails. Employees are advised to take screen prints of messages or web pages and be careful to record the time, date and place of the site

Adults may wish to seek the support of their trade union or professional association representatives or another colleague to support them through the process.

Adults are encouraged to report all incidents of cyberbullying to the Anti-Bullying Lead. All such incidents will be taken seriously and will be dealt with in consideration of the wishes of the person who has reported the incident. It is for the individual who is being bullied to decide whether they wish to report the actions to the police.

Adults should be familiar with the Anti-Bullying Policy and know what to do in the event that a child discloses that they are being cyber-bullied.

Apprendix A

Relevant Legal Framework:

Computer Misuse Act 1990 This Act makes it an offence to: • Erase or amend data or programs without authority; • Obtain unauthorised access to a computer; • "Eavesdrop" on a computer; • Make unauthorised use of computer time or facilities; • Maliciously corrupt or erase data or programs; • Deny access to authorised users.

Data Protection Act 1998 This protects the rights and privacy of an individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that personal data must be: • Fairly and lawfully processed; • Processed for limited purposes; • Adequate, relevant and not excessive; • Accurate; • Not kept longer than necessary; • Processed in accordance with the data subject's rights; • Secure; • Not transferred to other countries without adequate protection.

Freedom of Information Act 2000 The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003 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 purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988 It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000 It is an offence for any person to intentionally and without lawful authority to intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to: • Establish the facts; • Ascertain compliance with regulatory or self-regulatory practices or procedures; • Demonstrate standards which are or ought to be achieved by persons using the system; • Investigate or detect unauthorised use of the communications system; • Prevent or detect crime or in the interests of national security; • Ensure the effective operation of the system. • Monitoring but not recording is also permissible in order to: • Ascertain whether the communication is business or personal; • Protect or support helpline staff. • The provision reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994 This provides protection for Registered TradeMarks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trademarks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988 It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984 It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994 This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they: - • Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or • Display any writing, sign or other visible representation which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress. Racial and religious hatred act 2006 This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.
Protection from Harassment Act 1997 A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.
Protection of Children Act 1978 It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.
Sexual Offences Act 2003 The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) and you arrange to meet them or travel to meet them (anywhere in the world) with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in any sexual activity with any person under 18, with whom they are in a position of trust (typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.
Public Order Act 1986 This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007. Obscene publications act 1959 and 1964 Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.
The Human Rights Act 1998 This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the provision context, human rights to be aware of include: • The right to a fair trial • The right to respect for private and family life, home and correspondence • Freedom of thought, conscience and religion • Freedom of expression • Freedom of assembly • Prohibition of discrimination • The right to education These rights are not absolute. The provision is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.