

Families Fighting for Justice and O.L.L.Y (Our Lost Love Years)

Internet Policy

Internet acceptable use policy

Networked resources, including internet access, are potentially available to learners and staff at OLLY/FFFJ. All users are required to follow the conditions laid down in the policy. Any breach of these conditions may lead to withdrawal of the user's access; monitoring and or retrospective investigation of the user's use of services, and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

These networked resources are intended for educational purposes, and may only be used for legal activities consistent with the rules of KIND. Any expression of a personal view about OLLY/FFFJ or associates matters in any electronic form of communication must be endorsed to that effect.

Any use of the network that would bring the name of OLLY/FFFJ or associates into disrepute is not allowed.

OLLY/FFFJ expects that staff will use new technologies as appropriate within the curriculum and that staff will provide guidance and instruction to learners in the use of such resources. Independent learner users of the internet or will only permitted upon receipt of signed permission and agreement forms as laid out below. All computer systems will be regularly monitored to ensure that they are being used in a responsible fashion

CONDITION OF USE

Personal Responsibility

Access to the networked resources is a privilege, not a right. Users are responsible for their behaviour and communications. Staff and learners will be expected to use the resources for the purposes for which they are made available. Users are to take due care with the physical security of hardware they are using. Users will accept personal responsibility for reporting any misuses of the network to the management.

NETWORK ETIQUETTE AND PRIVACY

Users are expected to abide by the rule of network etiquette. These rules include but are not limited to the following:

1. Be polite – never send or encourage others to send abusive messages
2. Use appropriate language – users should remember that they are representatives of OLLY/FFFJ on a global public system. Illegal activities of any kind are strictly forbidden
3. Do not use language that could be calculated to incite hatred against any ethnic, religious or other minority group
4. Privacy – do not reveal any personal information (e.g home address, telephone number) about yourself or other users. Do not trespass into other user's. Do not trespass into other users' files or folders

INTERNET ACCEPTABLE USE POLICY

1. Password – do not reveal your password to anyone. If you think someone has learned your password then contact Peter Dunning.
2. Electronic mail – is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities Do not send anonymous messages
3. Disruptions – do not use the network in any way that would disrupt use of the network by others.
4. Learners will not be allowed access to unsupervised and/or unauthorised chat rooms and should not attempt to gain access to them
5. Staff and learners finding unsuitable websites through the KIND network should report the web address to the management.
6. Do not introduce floppy disks or pen drives into the network without having them checked for viruses.
7. Do not attempt to visit websites that might be considered inappropriate. (Such sites visited leave evidence on the computer. Downloading some material is illegal and the police or other authorities may be called to investigate such use)
8. Unapproved system utilities and executable files will not be allowed in learners' work areas or attached to e-mail.
9. Files held on the KINDS network will be regularly checked by the staff.
10. It is the responsibility of the User (where appropriate) to take all reasonable steps to ensure compliance with the conditions set out in this Policy document, and to ensure that unacceptable use of the Internet/Intranet does not occur

UNACCEPTABLE USE

Examples of unacceptable use include but are not limited to the following:

Users must login with their own user ID and password, where applicable, and must not share this information with other users. They must also log off after their session has finished

Users finding machines logged on under other users username should log off the machine whether they intend to use it or not

Accessing or creating, transmitting, displaying or publishing any material (e.g images, sounds or data) that is likely to cause offence, inconvenience or needless anxiety

Accessing or creating, transmitting or publishing any defamatory material.

Receiving, sending or publishing material that violates Data Protection Act or breaching the security this act requires for personal data

Transmitting unsolicited material to other users (including those on other networks)

Unauthorised access to data and resources on the KIND network system or other systems

User action that would cause corruption or destruction of other users' data, or violate the privacy of other users, or intentionally waste time or resources on the network or elsewhere

INTERNET ACCEPTABLE USE POLICY

Additional Guidelines

1. Users must comply with the acceptable use policy of any other networks that they access
2. Users must not download software without approval from staff

SERVICES

There will be no warranties of any kind, whether expressed or implied, for the network service offered by KIND. KIND will not be responsible for any damages suffered while on the system. These damages include loss of data as a result of delays, non deliveries, or service interruptions caused by the system or your errors or omissions. Use of any information obtained via the network is at your own risk

NETWORK SECURITY

Users are expected to inform the management immediately if a security problem is identified. Do not demonstrate this problem to other users. Users must login with their own user id and password, where applicable, and must not share this information with other users. Users identified as a security risk will be denied access to the network

PHYSICAL SECURITY

Staff users are expected to ensure that portable ICT equipment such as laptops, digital still and video cameras are securely locked away when they are not being used. Items that need to be left over breaks and lunchtimes for example will need to be physically protected by locks and or alarms

WILFUL DAMAGE

Any malicious attempt to harm or destroy any equipment or data of another user or network connected to the KIND system will result in loss of access, disciplinary action and if appropriate, legal referral. This includes the creation or uploading of computer viruses. The use of software from unauthorised sources is prohibited.

MEDIA PUBLICATIONS

Written permission from parents or carers will be obtained before photographs of learner or published. Named images of learners will only be published with the separate written consent of their parents or carers.

Publishing includes, but is not limited to:

- The OLLY/FFFJ website
- The Local Authority web site,
- Web broadcasting
- TV presentations
- Newspapers

Learners' work will only be published (e.g. photographs, videos, tv presentations, web pages etc) if parental consent has been given