Acceptable Usage Policy for Staff

Introduction

Access to email and internet should be granted by The Education Fellowship on the basis of justifiable educational or business need acceptable to line managers.

Staff should read and **sign** this Acceptable Usage Policy before being given access to use the internet or email at work.

This policy must be viewed annually by all staff if any changes are made to the policy since the original signing of the Acceptable Usage policy.

The academy must keep a register of all staff to indicate that they have read, understood and agree to abide by the policy.

Staff must:

- agree to The Education Fellowship viewing, where there are reasonable suspicions of misuse, any emails they send or receive, material they store on The Education Fellowship's computers, or logs of websites they have visited
- only access those services they have been given permission to use
- not access the internet or email for non-business purposes, unless agreed by the line manager
- ensure all work/activity on the internet and email is directly related to their work
- not give their password or login name to anyone
- not download, use or upload or send by email any material which, in doing so, infringes copyright
- not view, upload, download or send by email any content which is likely to be unsuitable for an educational establishment. This applies to any material of a violent, dangerous, racist, or inappropriate sexual content. If a staff member is ever unsure about this point, or the suitability of any content, they should consult their line manager.
- not use strong language, abusive language or aggressive behaviour
- not write anything on a website or send by email anything which is personally abusive

Monitoring and Sanctions

Penalties for misuse of computer systems will depend on the nature and seriousness of the offence. Disciplinary action may be taken against staff who contravene this policy.

The Education Fellowship, for various legitimate business practices, may need to monitor the use of staff email and internet access from time to time to:

- establish the existence of facts (e.g. the details of an agreement made)
- monitor for quality control and staff training purposes
- prevent or detect crime
- investigate or detect unauthorised use of The Education Fellowship's ICT systems (including email and internet)
- intercept for operational purposes, such as protecting against viruses and making routine interruptions, such as forwarding email to correct distributions
- gain access to routine business communications (e.g. checking email) when staff are on holiday or sick leave

In addition:

- The Education Fellowship may monitor, without notice and with justification, external and internal email and internet usage, including length of use and sites visited. It has the right, if it wishes, to access any content sent or received by the user
- The Education Fellowship may monitor and assess online content to ensure staff comply with ICT policy - in particular to prevent the use of computer resources for discriminatory purposes or harassment, and/or committing a criminal offence. This must be communicated in writing to all staff and other people who may have access to The Education Fellowship ICT systems
- Should an employee have their access to the internet and email withdrawn, with or without notice, they can appeal against this decision through the grievance procedure

Scope of staff email and internet acceptable use policy

The Acceptable Usage Policy will:

- apply to all employees, employment agency staff and contractors and other users who have access to internal/external email and/or the internet

- may also apply to visitors, including family members, and cover staff as appropriate
- be modified as necessary to enable ICT technical/support staff to perform their duties as directed
- apply to all access to the internet and use of email using computers owned or operated by The Education Fellowship or brought onto its premises, whether accessed during normal working hours or not

Responsibilities

Line managers are responsible for ensuring their staff, agency and contract staff are made fully aware of the staff AUP.

The IT Department is responsible for providing line managers with appropriate information on policy compliance.

Restrictions on staff use of school IT

Internet and email access is provided for business purposes. However, limited and responsible personal use may be permitted at the line manager's discretion, provided it takes place during breaks or personal time. In particular:

- Users must understand that privacy is not guaranteed and restrictions to non-business internet sites may be applied
- Any personal data created or accessed by staff through email, the internet or through any computer programme may be viewed or accessed by the academy without their permission
- The Education Fellowship IT systems must not be used for conveying messages that may be considered defamatory, derogatory, obscene, discriminatory or are otherwise abusive or inappropriate
- Harassment is a serious offence that will be dealt with through the Disciplinary Procedure and Anti-Harassment and Bullying ('Dignity at Work') Procedure
- Any inappropriate material inadvertently received by email which may cause offence to others must be reported to the user's line manager. The definition of 'inappropriate material' for the purposes of this policy is anything which could potentially be illegal or personally abusive
- Staff should not issue The Education Fellowship web addresses to any site that is filtered by The Education Fellowship and therefore is

intentionally inaccessible from The Education Fellowship network (e.g. some social networking sites)

- Staff should be made aware that issuing work email addresses to companies may generate excessive junk mail
- Under no circumstances should material received from an internal or external source, which is not strictly for business purposes, be passed on to any other system user or to any other email address. It must not be stored on any network drive, local drive or removable media
- Defamation is the publication of a statement that adversely affects a person's or an organisation's reputation, for which legal action may be taken against the sender. Users must not send or circulate negative information about an individual or organisation without first checking that the contents are accurate, and obtaining permission from their line manager
- Defamation of The Education Fellowship would be seen as a breach of an employee's contract of employment
- Use of digital information carries with it a risk of breach of confidence. Staff must be aware of their obligations under The Education Fellowship guidance with respect to personal and sensitive data, and commercially or otherwise confidential information. Such information must not be transmitted by email or the internet
- Viewing, circulating, or downloading pornographic material on The Education Fellowship premises or using The Education Fellowship - owned equipment is a serious abuse of this policy and will be dealt with under the Disciplinary Procedure as gross misconduct
- Viewing of illegal material by staff must be reported to the police
- Users must ensure that copyright laws are not infringed by the downloading or circulation of material from the internet

The Education Fellowship does not accept liability for any personal loss or damage incurred through using The Education Fellowship IT resources for private use.

The Education Fellowship will review policies at regular intervals In the light of changes in the business, technology, legislation or relevant standards, and communicate the changes.

Legislation

The Education Fellowship promotes the highest standards of good practice and security in the use of information technology, and expects the highest

levels of integrity in its staff. In exceptional circumstances, where there are reasonable grounds to suspect that an employee has committed a serious criminal offence, the police will be informed.

Amongst others, the following legislation applies to the use of The Education Fellowship resources:

- Regulation of Investigatory Powers Act 2000
- Computer Misuse Act 1990
- Protection from Harassment Act 1997
- Sex Discrimination Act 1975
- Race Relations Act 1976
- Disability Discrimination Act 1995
- Obscene Publications Act 1959
- Telecommunications Act 1984
- Protection of Children Act 1978
- Criminal Justice Act 1988
- Data Protection Act 1998
- The Patents Act 1977
- Copyright, Designs and Patents Act 1988
- Defamation Act 1996
- Freedom of Information Act 2000
- Human Rights Act 1998.

Disciplinary Issues

Examples of behaviours which may require the use of The Education Fellowship disciplinary policy include:

- criminal acts, for example in relation to child abuse images
- visiting pornographic sites on The Education Fellowship premises or using The Education Fellowship equipment
- harassment in the form of deliberately and personally abusive emails or printed emails sent to a colleague, even if sent as a joke. Harassment can take a number of forms and is defined as unwanted conduct that affects the dignity of people within the workplace
- obscene, racist jokes or remarks which have been shared internally and externally and which may reflect on the image of employer and bring the organisation into disrepute
- downloading and installation of unlicensed products
- viewing non-pornographic but sexually explicit materials, except where this forms an authorised part of the employee's job (for example to support the teaching of A-level biology)

- unauthorised use of chat rooms or social networking sites, especially for sexual discourse or to make arrangements for sexual activity
- violation of The Education Fellowship's other legal obligations such as software media counterfeiting or illegitimate distribution of copied software
- The Education Fellowship has the right to monitor employees' or students' use of computer equipment where there is evidence to suggest misuse (Regulation of Investigatory Powers Act 2000)

Data security

- Confidential information held on The Education Fellowship computer systems may only be accessed with proper authorisation and if the information is pertinent to The Education Fellowship work
- Under no circumstances should personal or other confidential information held on computer be disclosed to unauthorised persons
- The unauthorised access to and/or unauthorised modification of data is a criminal offence under the Computer Misuse Act 1990
- Where possible, data must be stored on a network drive that is regularly backed up
- Data not stored on a network drive must also be regularly backed up
- Any mobile storage devices such as laptops, USB data sticks/pen drives or external hard disks should be appropriately encrypted
- Care should be taken when using mobile storage devices to ensure that personal, confidential information or sensitive corporate data are not taken off-site unless protected securely by passwords or encryption
- If the data network is used for the transmission or storage of CCTV images, then care should also be taken to ensure that legal requirements are met

I agree to the follow the guidelines of the Acceptable Usage Policy for Staff as described above.

Name……..

Academy……..

Date……