EHA INTERNET, EMAIL & COMPUTER SECURITY POLICY

INTRODUCTION

This policy applies to all staff and any others, both voluntary and paid, working on the premises and/or under auspices. This policy has been developed to protect the EHA's interests whilst ensuring the Internet & e-mail services are being used effectively and productively in a secure environment as well as providing guidelines to assist employees in the proper use of the EHA's facilities.

The EHA provides access to the information resources of the Internet to help employees undertake their roles and to be well informed. Internet & e-mail services provided by the EHA are regarded as essential business tools and are provided in order to enhance employees' performance and not as a benefit of employment.

Using such services improperly can result in both the EHA and the individual being open to legal sanction and it is therefore essential that all users ensure that they are aware of this policy and their own responsibilities under it. Inappropriate use of the EHA's communication systems, whether under this policy or otherwise, may lead to disciplinary action being taken against employees. Such misconduct may result in disciplinary sanctions being applied including in serious cases, dismissal.

The policy applies to all EHA and personal computer equipment (PC's, laptops, palmtops, PDA's, mobile phones, removable drives, etc.) connected to the EHA's Network, Internet and e-mail services, whether in the office or working remotely.

Definitions

Certain terms or definitions used in this policy should be understood to include related concepts for example:

a) "EHA" includes any affiliates and any subsidiaries or offices.
b) "Workplace" includes work undertaken at the EHA's and its customers'/members' premises and extends to the employee's home where the employee utilises and / or accesses the EHA's Internet and e-mail services.
c) "Document" covers any type of file that can be read on a computer screen as if it were a printed page, including HTML files read in an Internet browser, any file meant to be accessed by a word processing or desktop publishing program or its viewer, or the files prepared for Adobe Acrobat reader and other electronic publishing tools.
d) "Graphics" includes photographs, pictures, animations, movies, or drawings.
e) "Display" includes monitors, flat-panel active or passive matrix displays, monochrome LCDS, projectors, televisions and virtual-reality tools.

General Principles

a) All information relating to the EHA and its business operations are confidential. Employees must treat the EHA's paper-based and electronic information with utmost care.
b) When using e-mail, all expressions of fact, intention and opinion may

legally bind the employee and / or the EHA. The same principles apply to information exchanged in this way as those under the terms of your employment contract regarding other means of communication. For example, sending defamatory, sexist or racist jokes or other material are grounds for an action for defamation, harassment or incitement to racial hatred in the same way as making defamatory, sexist or racist comments to a colleague.

c) Employees should be aware that storing personal details on a computer file is subject to the Data Protection Act. Employees storing such information must inform their manager to ensure that there is a record of this with the Data Protection Registrar.
d) Employees should not use the Internet or e-mail for any purposes, which would be subject to disciplinary or legal action. If in doubt about a course of action, they should take advice from their manager.
e) Employees must exercise due care when collecting, processing or disclosing any personal data and only process personal data on behalf of the EHA where it is necessary to undertake their duties.
f) Encryption should not be used for any EHA related communications without prior authorisation from a line manager.
g) On-line Internet or e-mail accounts created for business purposes require that usernames and associated passwords be disclosed to the employees' line manager.
h) All material, which you intend to load onto any Company system via any attached peripheral (floppy drive, CD-ROM, Zip drives etc), should first be virus-checked. Virus protection software installed on company laptops and PC's should not be disabled under any circumstances unless expressly agreed with a line manager. If a virus is detected, all work on the PC must cease and a line manager notified immediately. Files that are open shouldnot be saved nor should the employee try to close down an 'at risk' computer - this may cause more damage if a virus is present.
i) Employees are required to take reasonable steps to ensure the security and safe keeping of all equipment when working on EHA premises and working remotely.
j) It is the responsibility of the employee to keep confidential their personal password(s).
k) In as far as it is possible employees should ensure that the PC issued to them remains clean from unauthorised URLs, cookies or downloaded images.

Rules For Use of the Internet
Employees are expressly prohibited from the doing any of the following, although this is not an exhaustive list:

a) Accessing the following categories or websites including:
    - Adult and sexually explicit (pornographic) sites.
    - Sites containing material which may offend others for example because of its racist or sexist content.
    - Sites promoting criminal acts and skills.
    - Sites promoting hate speech or violence.
    - Sites promoting illegal weapons.
    - On line games.
    - Pirate software sites.
    - Any site that places unnecessary burden on the EHA's infrastructure or which is contrary to International or UK law.

b) Using unauthorised personal computer equipment connected to the EHA's or its customers'/members' Internet & e-mail services.
c) Introducing packet-sniffing software (i.e. software which is used to intercept data on a network) or password detecting software unless it specifically relates to an employees' role within the EHA and has been authorised by a line manager.
d) Seeking to gain access to restricted areas of the EHA's or its customers'/members' networks.
e) Knowingly seeking to access data which an employee reasonably knows to be confidential unless authorised to do so.
f) Introducing any form of computer virus, worm, Trojan Horse or trap door programme code.
g) Using newsgroups without prior authorisation from a line manager.
h) Carrying out other illegal activities (for information, the following activities are criminal offences under the Computer Misuse Act 1990 – i) unauthorised access to computer material i.e. hacking, ii) unauthorised modification of computer material, iii) unauthorised access with intent to commit/facilitate the commission of further offences).

Should it become necessary to download any software, except from partner or supplier sites, employees must seek permission from their line manger or appropriate client authority who will determine that the source is safe and arrange for the files to be downloaded.

Rules for Use of E-Mail
The EHA's E-Mail system only should be used for all business related e-mail communications unless otherwise authorised by a line manager. Employees must not:

- Impersonate any other person when using e-mail or amend any messages received.
- Send any illegal e-mails. It is illegal to transmit material (including attachments) and statements which are:
  - Fraudulent or part of an unlawful activity.
  - Slanderous, libellous, defamatory, offensive, obscene, pornographic.
  - Abusive or threatening violence, incitement to break the law.
  - Harassment on any basis (including race, ethnic origin, nationality, religion, skin colour, sex or sexual orientation, disability or sensory impairment, HIV status).

Rules for Personal Use of the Internet & E-mail
Employees may use the Internet and e-mail services for personal use provided that it does not interfere with their duties and therefore should be restricted to outside normal working hours (before 9:00 am, during lunch breaks and after 5:30pm). Employees must observe any rules relating to personal use of the Internet and e-mail whilst working on customer/member premises.

Personal use of the Internet and e-mail must:

a) Comply with this policy.
b) Not be used for private commercial ventures (e.g. renting out a holiday cottage, selling personal property), but it may be used for domestic purposes and personal communications.
c) Not interfere with the performance of an employees' duties and is

generally restricted to use outside normal working hours Fifteen minutes of daily personal use would not be considered to be unreasonable during working hours although this type of access should be infrequent.

d) Does not damage, affect the performance of, or otherwise negatively impact the EHA's or its customers'/members' IT infrastructure.

MONITORING COMMUNICATIONS

a) The EHA maintains its right to inspect any and all files stored in private and or common access areas of its network, on individual computer hard drives as well as all removable discs (e.g. zip discs, floppy discs, CD-Rom Discs etc.).

The EHA may implement monitoring systems that help manage the use of its Internet and e-mail systems. Personal communications of a sensitive or confidential nature should not therefore be sent by email because it is not guaranteed to be private.

b) However it may be necessary to access and record an employees' business communications in certain circumstances, which includes the following:
- Provide evidence of business transactions.
- During periods of absence, managers may require access to employee business communications.
- Confirmation that business procedures are adhered to and monitoring standards of service.
- Maintaining the effective operation of the EHA's communication systems.
- Preventing or detecting unauthorised use of the EHA's communications systems or criminal activities.

c) **THE EHA** will not routinely monitor personal communications except for traffic and billing data at a network level and a high level of trust is placed on employees to observe the requirements of this policy, however if there is any evidence that this policy is being abused, the EHA reserves its right to investigate alleged breaches and take appropriate disciplinary action in accordance with the EHA's Disciplinary Procedures.

d) Employees should note that when visiting an internet site or creating / receiving an e-mail, unique ID's such as usernames and IP addresses may be recorded on the EHA's IT systems.

Copyright

The **Copyright, Design and Patents Act 1988** is applicable to all types of creations, including software programs, databases, text, graphics and sounds by an author or an artist. This will include any that are accessible through the EHA's computing facilities. Only software authorised by the EHA and for which a valid licence has been purchased should be installed on an EHA PC. Any uploading or downloading of information which is not authorised by the copyright owner or any substantive extraction of information from a database which is not authorized by the database owner will be deemed to be an infringement of their rights.

Some types of infringement give rise to criminal offences, the penalties for which may amount to a term of imprisonment or an unlimited fine. It is also possible for the copyright owner to claim compensation or to have infringing activities prevented by injunction.

Employees must not make, transmit or store an electronic copy of copyright material without the permission of the owner.

Security

Employees are required to observe the following:

a) PCs / Terminals should be logged off the network when left unattended for any period of time. They should be switched off on leaving in the evening. PC's holding sensitive data must have a password installed.

b) If employees are provided with computers which are portable in nature they must ensure that such computers, when not in use in the office or at home or when travelling are safeguarded against accident and theft when in transport. If left in a vehicle for any time they must be secured in a locked boot.

c) It is company policy to lock laptops in a secure place at night and ensure the keys are hidden appropriately.

d) Where employees are provided with User-ID's and passwords to access the EHA's computer systems, they must not disclose them to anyone, unless expressly directed to do so by a manager. Passwords must be kept secret, changed often, of a no-nonsense type and NOT such words as: family names, pet names, car registration no's. It is suggested that passwords are between eight and fifteen digits long and contain upper and lower case, numbers and symbols such as - % &.

e) In the event that employees encounter a computer virus, or suspect that they have, they should leave the computer as it is and immediately contact the Office Manager. Under no circumstances should the suspected infected computer be utilised.

f) Only the Systems Administrator can change or authorise changes to hardware or software configurations.

g) All data media e.g. floppy disks, tapes etc that are obsolete must be destroyed on site.

h) Users of portable and stand alone computers are responsible for the backup of data held and ensuring that adequate virus scanning software is in use.

i) Record playback facilities on the keyboards must not be used for log on procedures.

j) Program developers (inc. local databases) must not use live data for testing purposes. Program development must be kept separate from live use of the system.

k) Employees are responsible for keeping their PC / laptop in a good state of cleanliness and ensure that they are not adorned with unnecessary decoration. They should take all reasonable steps to ensure that computers and data media are not exposed to damage from spillages.

LEAVING THE COMPANY

On leaving the Company, employees are obliged to transfer and / or make available any documents relating to their day-to-day work or customers/members to their manager. Employees are responsible for deleting any personal information from the system and returning all company property in their possession to their line manager.