INTERNET AND ELECTRONIC MEDIA POLICY AND GUIDANCE - SCHOOL STAFF AND GOVERNORS

1. INTRODUCTION

1.1. The Internet and its facilities offer the greatest access to information and freedom of communication the world has ever seen. It gives every school a worldwide library, notice board and messaging system. Everyone is encouraged to make the maximum use of the resources the information revolution has given us.

1.2. Both staff and governors need to be aware of some of the problems which come with that freedom. There is disturbing and illegal material on the Internet and children are especially vulnerable to those who misuse the internet, as well as misusing it themselves.

1.3. Staff may never come across any of the problems described here during normal daily use of the Internet and shouldn't avoid using the Internet and the enormous advantages just because of them. The guidance is designed to help make staff aware of the small but significant risks, and to know how to deal with them. Some risks are obvious, but some are harder to spot. Similar advice is available for pupils and parents.

1.4. This policy relates to all Staff and Governors in school. It relates to desktop computers, laptops, phones with email and internet connections, personal organisers and any other item of equipment which may become available in the future which gives users the ability to access the internet or send and receive electronic messages.

1.5. Throughout the policy, the Chair of Governors should be the contact in cases relating to the Headteacher.

1.6. All use is subject to the relevant legislation which includes the Data Protection Act, Freedom of Information Act, Computer Misuse and Designs Act and Copyright and Patents Act.

1.7. Staff must adhere to this policy. Failure to follow it is a serious disciplinary matter which could lead to disciplinary action up to and including dismissal. It may also lead to criminal or civil action if illegal material is involved or legislation is contravened.

1.8. If a breach of the policy is of a very serious nature, the procedure in Appendix 1 must be used. Cases of a very serious nature include for example, all cases of accessing, creating, using, transmitting or encouraging material with content that is sexually or racially offensive, violent or involving abuse of children or other vulnerable groups.

1.9. If a breach of the policy is in connection with a safeguarding issue, the Local Authority Designated Officer (LADO) must be contacted on 023 9284 1220. Appendix 1 of this policy must be followed and also the Management of Allegations of Abuse procedure in the Manual of Personnel Practice.

2. GENERAL PRINCIPLES

2.1. Inappropriate use is explained in Paragraph 3.

2.2. The Internet, e-mail, message boards and newsgroups should be used responsibly and legally. Staff should not do anything that could expose pupils to any risks, interfere with the work of the school or bring the school into disrepute, cause offence, cause damage or jeopardise the security of data, networks, equipment or software, or break laws such as copyright, data protection or anti-discrimination legislation.

2.3. Schools should use service providers that block out unsuitable sites and offer a filtered service. Schools should also install software that limits access to unsuitable sites where practical. This does not make it impossible to misuse the Net, and schools should still monitor use by checking the computer itself, material produced on it, and responding to tip-offs and complaints about misuse.

2.4. Viruses can be introduced through file transfers and may cause damage to school systems. The school must have a procedure for checking downloaded files for viruses.

2.5. Pupils should be encouraged to use electronic media responsibly. Staff should also be vigilant about the use of electronic media by pupils and make every effort to minimise the risk of pupils being exposed to offensive and disturbing material.

2.6. If staff come across unsuitable sites, they should alert their Line Manager or Headteacher immediately.

2.7. The IT Network Manager may monitor usage of the Internet and email facilities and has access to reports on any Internet sites that have been visited. This is irrespective of whether it is for school or private use. Any potential misuse identified by the IT Network Manager in the course of their duties will be reported confidentially to the Headteacher.

2.8. If inappropriate use of the internet or electronic media is of a very serious nature, the procedure in Appendix 1 must be followed. This may lead to disciplinary action under the disciplinary policy up to and including dismissal.

2.9. For all other cases of inappropriate use of the internet and electronic media, the disciplinary policy may be used. In these circumstances, staff are advised to contact their Trade Union.

3. INAPPROPRIATE USE

3.1. There are various definitions of what inappropriate use of electronic media is. For some it will mean accessing pornography while for others it will include sending junk mail ("spam") or insulting, aggressive e-mails ("flame mail").

3.2. Inappropriate use includes :

- using electronic media for accessing, creating, using, transmitting or encouraging material which:
    - is obscene and/or illegal.
    - is pornographic in its nature.
    - is discriminatory.
    - is defamatory.
    - infringes another person’s copyright.
    - is offensive.
    - is frightening or disturbing to adults or children.
    - promotes illegal acts.
    - failed to adhere to the Internet and Electronic Media Policy and Guidance.

It can also include anything that:

- disrupts other users’ work in any way, including by viruses or data corruption.
- violates other people's privacy.
- involves the misuse of IT systems and data.
- involves use of unauthorised software (including games) or software that is being used without the relevant licence.

- knowingly introduces a software virus or anything that corrupts data.

- involves using chat rooms, social networking sites or similar services (other than those within the UniServity learning platform), unless the use has been approved by the Headteacher who has arranged specific access to be allowed for curriculum activities.

- transmits unsolicited commercial or advertising material.

- transmits or downloads confidential information.

- wastes network or staff resources.

- expresses personal views or opinions which could be misinterpreted as being those of the school.

- commits the school to purchase or acquire goods or services without proper authorisation.

- Involves illegal activities including breaching legislation such as the Data Protection, Freedom of Information, Computer Misuse and Design Copyright and Patents Acts.

This is not an exhaustive list but merely an indication of the types of conduct that could come under the heading of inappropriate use and could result in disciplinary action up to and including dismissal. In some cases criminal or civil prosecution could take place as well.

3.3. It is sometimes hard to tell if messages you send from school will be seen as junk mail, and many people are confused about the legality of copying pictures, software or music files. If in doubt, advice can be sought from the Information Service on 023 9283 4781.

4. OFFENSIVE AND ILLEGAL MATERIAL

4.1. Most sites are perfectly safe but exploring electronic information may bring staff into contact with offensive material and even into contact with potentially dangerous people. Staff should be aware of the risks.

4.2. Offensive material is considered to be anything of a pornographic nature and material involving threats, violence, promoting illegal acts, racial or religious hatred or discrimination of any kind. It also covers material that the person knows or ought to have known would offend a colleague with particular sensitivities, even if the subject is not offensive in itself.

5. WHAT TO DO IF YOU FIND OBSCENE OR VIOLENT MATERIAL ON AN INTERNET SITE ACCIDENTALLY

5.1. Anyone who accidentally accesses offensive material should inform their Line Manager or Headteacher immediately. Accidental access will not result in disciplinary action but failure to report it may do so. The IT Network Manager may monitor usage of the Internet and email facilities and has access to reports on any Internet sites that have been visited.

5.2. Make a note of the address (the URL) of the page. If you don't know how to do this, you can find it in the address panel at the top of the screen, or by clicking on the file menu and then PROPERTIES.

5.3. Prevent anyone else - especially children - from seeing it. Press the "back" button on your browser to clear the screen temporarily without losing the data.

5.4. If you think the material is illegal, and especially if it relates to child pornography, you will need to inform the Headteacher who will assess the situation and may contact the Information Service on 023 9283 4781 and the Internet Watch Foundation (IWF) hotline on 01223 237700. The IWF monitors the Internet and asks for offensive sites to be removed. The IWF can also alert the police when necessary. They will need to know what the site contains and its address (the URL).

5.5. The Headteacher will note the details of the access and the details of the individual reporting it.

5.6. If a member of staff is upset or disturbed by accidentally viewing highly offensive material, they can seek confidential counselling from The Oakdale Centre on 0800 027 7844 or Teacher Support Line on 0800 056 2561.

5.7. Employees may wish to contact a representative from their Trade Union.

6. E-MAIL AND FAXES

6.1. This section applies to email, faxes and any form of electronic messaging and attachments.

6.2. Despite the speed and ease of use, electronic communication and information should be treated the same way as that on paper. The same ethical standards should apply.

6.3. Confidential information that you might hesitate to send on paper should not be sent electronically. Neither e-mails nor faxes are

"secure" systems, they can end up going to the wrong person very easily.

6.4. Care should be taken when sending emails to ensure they are not seen as offensive, threatening, defamatory and do not contain illegal material. As far as the law is concerned, e-mails are published material, therefore it is possible to defame or libel someone in an e-mail or electronic fax in the same way as you could in a letter. If this material ends up in the public domain it can result in expensive legal action. Any member of staff who receives this type of email may wish to speak to their Line Manager or Headteacher regarding the matter depending on the individual circumstances.

6.5. Emails can be easily misunderstood. Emotional meaning may be lost in text and humour can easily be misinterpreted. Emails should be unambiguous and use plain English.

6.6. Users should not re-send email chain letters and should use caution with any email that asks the reader to forward it to others. If in doubt the Headteachers advice must be sought.

6.7. If a member of staff has been given access to another person's in-box to check mail when they are unable to do so themselves, they must not use this access at any other time without their permission.

7. SOCIAL NETWORKING SITES AND NEWSGROUPS

7.1. The School will normally block/filter access to social networking sites (other than those within the 'UniServity' learning platform), unless short term access is required for a specific curriculum activity.

7.2. Newsgroups may be blocked unless a specific use is approved.

8. PRIVATE USE OF INTERNET AND E-MAIL FACILITIES USING SCHOOL EQUIPMENT.

8.1. Any private use of Internet and email facilities using school equipment is at the discretion of the Headteacher. If occasional private use is agreed, staff will need to comply with the following.

- It must not interfere with the work of the school.
- It must not be related to an outside business interest.
- It must not involve the use of chat rooms, social networking sites or similar services (other than those within the UniServity learning platform).

- It must comply with this policy, including the provisions regarding inappropriate use and offensive and illegal material.

8.2. Access to web-based mail is at the discretion of the Headteacher.

8.3. Newsgroups should not be used without prior approval of the Line Manager/Headteacher.

8.4. Users posting information to newsgroups (with prior approval from the Line Manager/Headteacher) should not make any statement, or disclose any information that could bring the school into disrepute.

8.5. Line Managers should monitor time spent on private use. Excessive use may lead to withdrawal of access or disciplinary action up to and including dismissal.

9. ADVICE FOR USE OF CHAT ROOMS, SOCIAL NETWORKING SITES AND OTHER SIMILAR SERVICES OUTSIDE OF THE WORKPLACE

Staff should take care when using chat rooms, social networking sites or similar services outside of the workplace as information is not secure and could be accessed by others and used in a detrimental way.

10. CYBERBULLYING

10.1. Cyberbullying may include bullying via mobile phone, email or by discriminatory or defamatory comments posted on internet websites, chat rooms, social networking sites or similar services.

10.2. If a member of staff believes that cyberbullying has occurred, they should report it to their Line Manager or Headteacher (or Chair of Governors in the case of the Headteacher). Cyberbullying could be an individual incident or a prolonged issue, either in school or out of school. It may be in relation to a pupil, another employee or an unknown source. Depending on the circumstances, the issue may be initially dealt with in accordance with the Dignity at Work policy or the school procedure for pupils.

10.3. The Headteacher/Chair of Governors should liaise with the Schools Human Resources Team and Internal Audit/Information Service when an allegation of cyberbullying by a member of staff is raised. Cyberbullying by an employee may lead to disciplinary action, up to and including dismissal.

10.4. The Headteacher/Chair of Governors should liaise with Internal Audit/ Information Service regarding incidents of cyberbullying by pupils.

10.5. In cases of actual or suspected illegal content relating to cyberbullying, the Headteacher/Chair of Governors should contact Internal Audit who will liaise with the police as necessary.

10.6. The DCSF Guidance – Cyberbullying - Supporting School Staff provides advice for having offensive content removed. It is available at www.teachernet.gov.uk/wholeschool/behaviour/cyber/

10.7. Support can be provided by Teacher Support Line – 0800 056 2561 or The Oakdale Centre – Confidential Counselling 0800 027 7844

10.8. Other useful contacts for support are available in Section 13 of this policy.

11. WHAT TO DO IF INAPPROPRIATE USE OF THE INTERNET OR ELECTRONIC MEDIA IS SUSPECTED.

11.1. Any information regarding suspected inappropriate use of the internet and electronic media must be reported immediately to the Headteacher in a confidential manner.

11.2. The Headteacher will consider the information. If a breach of the policy is of a very serious nature the procedure in Appendix 1 must be used. Cases of a very serious nature include for example, all cases of accessing, creating, using, transmitting or encouraging material with content that is sexually or racially offensive, violent or involving abuse of children or other vulnerable groups.

11.3. If a breach of the policy is in connection with a safeguarding issue, the LADO must be contacted on 023 9284 1220 and the Management of Allegations of Abuse procedure followed in conjunction with Appendix 1.

11.4. If the inappropriate use is of a less serious nature, the headteacher may consider disciplinary action up to and including dismissal.

12. MONITORING

12.1. The IT Network Manager may monitor usage of Internet and email facilities and has access to reports on any Internet sites that have been visited. This is irrespective of whether it is for school or private use.

12.2. Any potential misuse identified by the IT Network Manager in the course of their duties must be reported to the Headteacher immediately. Misuse may lead to disciplinary action, up to and including dismissal.

13. USEFUL CONTACTS

The Schools Human Resources Team
023 9268 8337

Local Authority Designated Officer (LADO) – (For an allegation in connection with a safeguarding issue)
023 9284 1220

Internal Audit (Serious inappropriate use of the internet and electronic media)
023 9283 4697

The Information Service,
023 9283 4781 (Net monitoring, Software, Security)

Merefield House,
023 9283 9111

Legal Services (Copyright and software fraud)
023 9283 4935

Internet Watch Foundation (IWF) hotline on 01223 237700
or www.iwf.org.uk

Teacher Support Line – 0800 056 2561

The Oakdale Centre – Confidential Counselling 0800 027 7844

Further information is available on the following websites:

Portsmouth Connected Learning Community

www.portsmouthclc.portsmouth.gov.uk

Direct link to Kent County Council advice and guidance - working with Becta.

http://www.portsmouth-learning.net/index.cfm?s=1&m=1&p=1,home_page_item&id=115

The Child Exploitation and Online Protection Centre (CEOP)

www.ceop.gov.uk

DCSF Guidance – Cyberbullying - Supporting School Staff

www.teachernet.gov.uk/wholeschool/behaviour/cyber/

APPENDIX 1

VERY SERIOUS BREACH OF THE INTERNET AND ELECTRONIC MEDIA POLICY AND GUIDANCE

PROCEDURE FOR HEADTEACHERS OR THE CHAIR OF GOVERNORS TO FOLLOW

1. INTRODUCTION

1.1. If the Headteacher (or a senior member of staff if the Headteacher is likely to be the decision maker in a potential disciplinary case at a later date) considers that a member of staff is involved in a **very serious breach** of the Internet and Electronic Media Policy and Guidance they must use this procedure. In the case of a Headteacher, the Chair of Governors will use this procedure.

1.2. For all other cases of inappropriate use of the internet and electronic media, the disciplinary policy may be followed.

1.3. The Disciplinary Policy can be found in Section 3 of the Manual of Personnel Practice.

2. VERY SERIOUS BREACH

A very serious breach of the policy might include, for example, cases of accessing, creating, using, transmitting or encouraging material with content that is sexually or racially offensive, violent or involving abuse of children or other vulnerable groups.

3. ACTION TO TAKE FOR A VERY SERIOUS BREACH

3.1. If a breach of the policy is in connection with a safeguarding issue, the Local Authority Designated Officer (LADO) must be contacted immediately on 023 9284 1220.

3.2. If a breach of the policy is in connection with a safeguarding issue the Management of Allegations of Abuse procedure (including consideration of suspension) in the Manual of Personnel Practice must also be followed.

3.3. The Schools Human Resources Team should also be contacted for advice immediately.

3.4. Do not alert the member of staff until advised to do so.

3.5. Do not touch or move equipment. Evidence needs to be preserved in case of criminal activity.

3.6. The Schools Human Resources Team will contact Internal Audit who will advise on the case.

3.7. Internal Audit will liaise with the school and the Schools Human Resources Team and complete a confidential investigation.

3.8. Internal Audit may want to remove the PC for forensic examination. The PC should not be shut down or disconnected by anyone else.

3.9. If necessary, Internal Audit may liaise with the police for advice on any suspected criminal content.

3.10. Internal Audit will alert Social Care when necessary.

3.11. The Schools Human Resources Team will advise the Headteacher if the Suspension policy should be followed in conjunction with this procedure.

3.12. At any stage of the procedure the member of staff may be accompanied by a representative from their Trade Union or work colleague.

3.13. The member of staff's desk and area may need to be searched. If possible, this should be completed in their presence. Items taken must be listed and signed for by the member of staff or their representative.

3.14. The investigation may lead to disciplinary action up to and including dismissal.

