

Infringements and Sanctions APPENDIX 3

How will infringements be handled?

Whenever a student or staff member infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of the school leadership team.

The following are provided as exemplification only:

Students

Category A infringements

- Use of non-educational sites during lessons
- Unauthorised use of email
- Unauthorised use of mobile phone (or other new technologies) in lessons e.g. to send texts to friends
- Use of unauthorised instant messaging / social networking sites

*[Possible Sanctions: **referred to class teacher / tutor / senior manager / e-Safety Coordinator**]*

Category B infringements

- Continued use of non-educational sites during lessons after being warned
- Continued unauthorised use of email after being warned
- Continued unauthorised use of mobile phone (or other new technologies) after being warned
- Continued use of unauthorised instant messaging / chatrooms, social networking sites, NewsGroups
- Use of Filesharing software e.g. Napster, Vanbasco, BitTorrent, LiveWire, etc
- Accidentally corrupting or destroying others' data without notifying a member of staff of it
- Accidentally accessing offensive material and not logging off or notifying a member of staff of it

*[Possible Sanctions: **referred to Class teacher/ Course Director / Head of School / e-safety Coordinator** / removal of Internet access rights for a period / removal of phone until end of day / contact with parent]*

Category C infringements

- Deliberately corrupting or destroying someone's data, violating privacy of others
- Sending an email or MSN message that is regarded as harassment or of a bullying nature (one-off)
- Deliberately trying to access offensive or pornographic material
- Any purchasing or ordering of items over the Internet
- Transmission of commercial or advertising material

*[Possible Sanctions: **referred to Class teacher / Head of School / e-safety Coordinator / Principal / removal of Internet and/or Learning Platform access rights for a period / contact with parents / removal of equipment**]*

Other safeguarding actions

If inappropriate web material is accessed:

1. Ensure appropriate technical support filters the site
2. Inform LA as appropriate

Category D infringements

- Continued sending of emails or MSN messages regarded as harassment or of a bullying nature after being warned
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
- Bringing the school name into disrepute

*[Possible Sanctions – **Referred to Principal / Contact with parents / possible exclusion / removal of equipment / refer to Community Police Officer / LA e-safety officer**]*

Other safeguarding actions:

1. Secure and preserve any evidence
2. Inform the sender's e-mail service provider

Staff

Category A infringements (Misconduct)

- Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.
- Misuse of first level data security, e.g. wrongful use of passwords
- Breaching copyright or license e.g. installing unlicensed software on network

[Sanction - referred to Line Manager / Principal. Verbal Warning given.]

Category B infringements (Misconduct)

- Accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;

[Sanction - referred to Line Manager / Principal. Written/Verbal Warning given.]

Category C infringements (Gross Misconduct)

- Serious misuse of, or deliberate damage to, any school / Council computer hardware or software;
- Repeated infringements of Category B;
- Accessing or storing inappropriate images of children;
- Any deliberate attempt to breach data protection or computer security rules;
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988;
- Bringing the school name into disrepute.

[Sanction - Referred to Principal / Governors and follow school disciplinary procedures; report to LA Personnel/ Human resources, report to Police]

Other safeguarding actions:

- Remove the PC to a secure place to ensure that there is no further access to the PC or laptop.
- Instigate an audit of all ICT equipment by an outside agency, such as the schools ICT managed service providers - to ensure there is no risk of pupils accessing inappropriate materials in the school.
- Identify the precise details of the material.

If a member of staff commits an exceptionally serious act of gross misconduct they should be instantly suspended. Normally though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken.

Schools are likely to involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and data evidence, the Local Authority Human Resources team.

Child Pornography found?

In the case of Child Pornography being found, the member of staff should be **immediately suspended** and the Police should be called.

Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP):

http://www.ceop.gov.uk/reporting_abuse.html

How will staff and students be informed of these procedures?

- They will be fully explained and included within the school's e-safety / Acceptable Use Policy. All staff will be required to sign the school's e-safety Policy acceptance form;
- Pupils will be taught about responsible and acceptable use and given strategies to deal with incidents so they can develop 'safe behaviours'. Pupils will sign an age appropriate e-safety / acceptable use form;
- The school's e-safety policy will be made available and explained to parents, and parents will sign an acceptance form when their child starts at the school.
- Information on reporting abuse / bullying etc will be made available by the school for pupils, staff and parents.
- Staff are issued with the 'What to do if?' guide on e-safety issues, (see LGfL safety site).