Fyling Hall School
ICT Misuse Sanctions

How the school will respond to issues of misuse.

(Posters explaining the following sanctions are displayed in the ICT classroom and the staffroom.)

The following are provided for the purpose of example only. 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 Headmaster and Trustees.

Students:

Level 1 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 CL/ e-safety Manager /removal of phone until end of day / contact with parent/ removal of Internet access rights for a period

Level 2 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
- Accidentally accessing offensive material and not notifying a member of staff of it

Possible Sanctions: referred to CL / e-safety Manager / Head of House / removal of phone until end of week / contact with parent/ removal of Internet access rights for an extended period/ exclusion

Level 3 infringements

- Deliberately corrupting or destroying someone's data, violating privacy of others
- Sending an email 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 CL / e-safety Manager / Principal / contact with parents / removal of equipment/ removal of Internet and/or Learning Platform access rights for an extended period/ exclusion/ referral to police.

Level 4 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
- Deliberate acts to compromise or damage the school network
- 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 e-safety Manager/ Principal /exclusion / removal of equipment / referral to police / LA e-safety officer

Staff:

Level 1 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 / Warning given.

Level 2 infringements (Gross Misconduct)

- Serious misuse of, or deliberate damage to, any school computer hardware or software;
- 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 Academy into disrepute.

Sanction: referred to Headmaster and follow school disciplinary procedures / Police/ GTC/ Governors

Child Pornography:

In the case of child pornography being found, the member of staff will be immediately suspended and the Academy disciplinary procedures implemented.

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 to ensure there is no risk of pupils accessing inappropriate materials in the school.
Identify the precise details of the material.
Where appropriate, involve external agencies as part of these investigations.

How will staff and students be informed of these procedures?

Procedures are included within the school's e-safety / Acceptable Use Policy. All staff are required to sign the school's e-safety Policy acceptance form;
Pupils will be instructed about responsible and acceptable use and given strategies to develop 'safe behaviours'. Pupils are required to sign an age appropriate e-safety / acceptable use form;
The school's e-safety policy will be made available to parents who are required to sign an acceptance form when their child starts at the school.
Staff are issued with the 'What to do if?' guide on e-safety issues.

Updated January 2017 by S Allen To be reviewed by January 2018