Online-Safety Policy Infringement Procedures:

Policy: How will infringements be handled?

Whenever a student or staff member infringes the Online-Safety Policy, the final decision on the level of sanction will be at the discretion of the school management and will reflect the school's behaviour and disciplinary procedures.

STUDENT	
Category A infringements	**Possible Sanctions:**
• Use of non-educational sites during lessons • Unauthorised use of email and communications tools • Unauthorised use of mobile phone/personal device in lessons e.g. to send texts to friends • Use of unauthorised instant messaging / social networking sites	**Refer to class teacher / tutor** Escalate to: senior manager / Online-Safety Coordinator
Category B infringements	**Possible Sanctions:**
• Continued use of non-educational sites during lessons after being warned • Continued unauthorised use of email and communication tools after being warned • Continued unauthorised use of mobile phone/personal device after being warned • Continued use of unauthorised instant messaging / social networking sites, Games sites • Use of Filesharing software e.g. BitTorrent, for illegal downloading • Accidentally corrupting or destroying others' data without notifying a member of staff of it • Accidentally accessing offensive material and not notifying a member of staff of it	**Refer to Class teacher/ Head of Department / Year tutor / Online-Safety Coordinator** Escalate to: removal of Internet access rights for a period / removal of phone until end of day / contact with parent]

STUDENT	
Category C infringements	**Possible Sanctions:**
• Deliberately corrupting or destroying someone's data, violating privacy of others or posts inappropriate messages, videos or images on a social networking site. • Sending an email or message that is regarded as harassment or of a bullying nature (one-off) • Trying to access offensive or pornographic material (one-off) • Transmission of commercial or advertising material • Use of systems to circumvent schools online-safety tools such as VPN and proxy sites	**Refer to Class teacher / Year Tutor / Online-Safety Coordinator / Head teacher / removal of Internet and/or online services access rights for a period** Escalate to: contact with parents / removal of equipment **Other safeguarding actions if inappropriate web material is accessed:** Ensure appropriate technical support filters the site
Category D infringements	**Possible Sanctions:**
• Continued sending of emails or messages regarded as harassment or of a bullying nature Deliberately creating accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violentSharing or requesting of images or content of a minor that would be considered sexual or inappropriate. • 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	**Refer to Head Teacher / Contact with parents** **Other possible safeguarding actions:** • Secure and preserve any evidence • Inform the service provider if appropriate. • Liaise with relevant service providers/ instigators of the offending material to remove • Report to Police / CEOP where child abuse or illegal activity is suspected

STAFF	
Category A infringements (Misconduct)	**Possible Sanctions:**
• Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, social networking etc. • Not implementing appropriate safeguarding procedures. • Any behaviour on the World Wide Web that compromises the staff members professional standing in the school and community. • Lack of due care resulting in infection or distribution of viruses or malware • Misuse of first level data security, e.g. sharing of passwords. • Breaching copyright or license e.g. installing unlicensed software on network.	**Referred to line manager / Head teacher** Escalate to: *Warning given*
Category B infringements (Gross Misconduct)	**Possible Sanctions:**
• 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 creating ,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	**Referred to Head teacher / Governors;** **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. *Escalate to:eport to LA /LSCB, Personnel, Human resource.* Report to Police / CEOP where child abuse or illegal activity is suspected. ,

If a member of staff commits an exceptionally serious act of gross misconduct

The member of staff 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 abuse images found

In the case of Child abuse images 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

http://www.iwf.org.uk

How will staff and students be informed of these procedures?

- They will be fully explained and included within the school's Online-Safety / Acceptable Use Policy. All staff will be required to sign the school's online-safety acceptable use agreement 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 online-safety / acceptable use agreement form;
- The school's online-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 online-safety issues, (see LGfL safety site).

Sample agreement forms can be downloaded from the LGfL online-safety site