	Name of School	**Manor Primary School**
	Policy review Date	**September 2015**
	Date of next Review	**September 2018**
	Who reviewed this policy?	**Kate McGee & Petra Collins (HT & AHT/ICT Leader)**

Policy: 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 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 • Unauthorised use of mobile phone	**Refer to class teacher** Escalate to: senior teacher / e-Safety Coordinator
Category B infringements	**Possible Sanctions:**
• 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 • Use of Filesharing software e.g. Napster, Vanbasco, BitTorrent, LiveWire, etc • Trying to buy items online • 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	**Refer to Class teacher / e-safety Coordinator** Escalate to: removal of Internet access rights for a period / 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 MSN message that is regarded as harassment or of a bullying nature (one-off) • Trying to access offensive or pornographic material (one-off) • Purchasing or ordering of items online	**Refer to Class teacher / e-safety Coordinator / Head teacher / removal of Internet and/or Learning Platform 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 MSN messages regarded as harassment or of a bullying nature after being warned • Deliberately creating accessing, downloading or 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	**Refer to Head Teacher / Contact with parents** **Other possible safeguarding actions:** • Secure and preserve any evidence • Inform the sender's e-mail service provider. • 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, instant messaging etc. • Use of personal data storage media (e.g. USB memory sticks) without considering access and appropriateness of any files stored. • Not implementing appropriate safeguarding procedures. • Any behaviour on the internet that compromises the staff members' professional standing in the school and community. • Misuse of first level data security, e.g. wrongful use of passwords. • Breaching copyright or license e.g. installing unlicensed software on network.	**Referred to Headteacher** Escalate to: *Warning given*
Category B infringements (Gross Misconduct)	**Possible Sanctions:**
• Serious misuse of, or deliberate damage to, any school / Council 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 / Chair of 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:* *report to LA /LSCB, Personnel, Human resource.* Report to Police / CEOP where child abuse or illegal activity is suspected. ,

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 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 e-safety / acceptable use agreement 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.