Dunstable Icknield Lower School

Learn, Believe, Achieve

Digital Technology Risk Assessment – Dunstable Icknield Lower School

Assessment conducted by: Miss Strickler and Mrs Haynes	Job title: Computing Lead & Office Manager	Covered by this assessment: All staff, pupils, volunteers, and visitors Teachers, teaching assistants, volunteers, supervising adults, pupils.
Date of assessment: 6.12.19	Review interval: Annually	Date of next review: December 2020

Related documents		
Data Protection Policy Online Safety Policy	Health and Safety Policy First Aid Policy	Behavioural Policy Prevent Duty Policy

Risk rating		Likelihood of occurrence		
		Probable	**Possible**	**Remote**
Likely impact	**Major** Causes major physical injury, harm or ill-health.	High (H)	H	Medium (M)
	Severe Causes physical injury or illness requiring first aid.	H	M	Low (L)
	Minor Causes physical or emotional discomfort.	M	L	L

Potential risks	Risk rating prior to action H/M/L	Recommended controls	In place? Yes/No	By whom?	Risk rating following action H/M/L
Policies do not sufficiently cover the risks associated with digital technology	H	• Relevant policies, such as the Dunstable Icknield Lower School's Health and Safety Policy, Online Safety Policy, and Behavioural Policy, contain clear guidelines on how to manage any risks related to digital technology. • Relevant policies are regularly reviewed and updated where necessary, according to their respective review schedules. • Staff and pupils are trained in the risks associated with digital technology, both prior to first use, and refreshed on the risks whenever the advice is updated.	Y	Headteacher Computing Lead Office Manager	L
Staff/pupils do not know how to install, use or maintain the technology		• The technology comes with installation by IT technicians. Staff can install and maintain own technology in liaison with IT provider. • Staff and pupils are instructed on the correct use of any digital technology before using it for the first time, and at regular intervals thereafter. • 2nd INSET for staff each year allocated to training on technology used in school.	Y	Headteacher Computing Lead Office Manager IT technician	L
The technology is not installed, used or maintained correctly		• IT technicians to manage installations and ensure are maintained correctly. • Pre-installation checks are undertaken on the technology, to confirm that all the necessary components are included by IT technicians. • The technology is always used in accordance with its operating instructions, and staff/pupils are reminded of the proper procedures whenever it is apparent that the technology is not being used correctly. • Any incidents of improper use, whether by staff or pupils, are reported to the ICT coordinator.	Y	Computing Lead Office Manager IT technician	L
Electrical shock		• A pre-use check is conducted by the IT technicians and any electrical defects (e.g. exposed wiring) are dealt with immediately. • The technology is subject to annual PAT testing. • Defective technology is not used, and an out-of-order sign	Y	IT technician	L

Potential risks	Risk rating prior to action H/M/L	Recommended controls	In place? Yes/No	By whom?	Risk rating following action H/M/L
		is clearly displayed on the equipment for all to see.			
Fire/explosions		• The correct type of battery for any piece of digital technology is always used. • Batteries are never disposed of using fire. • Extension leads and adaptors are never overloaded. • Every piece of digital technology is annually PAT tested. • Defective technology is not used, and an out-of-order sign is clearly displayed on the equipment for all to see. • An established procedure is in place for dealing with any incidents of fire/explosions. • Pupils are advised to turn off, or discontinue using, a piece of digital technology whenever it overheats.	Y	IT technician Office Manager	L
Overloading of extension leads		• Only one adaptor per socket is used. • Adaptors are never plugged into other adaptors. • Block adaptors are never used. • Extension leads are annually PAT tested to check that their mechanisms are free and functioning.	Y	IT technician Office Manager	L
Eye strain		• Staff and pupils are encouraged not to sit close to their computers, and to give themselves a screen break every 20 minutes. • Staff are able to adjust display screen brightness to suit the surrounding lighting. • Staff are able to adjust text size so that it is comfortable to read. • Glare is reduced wherever possible, including through the use of anti-glare attachments for display screen equipment (DSE) screens or, for glasses wearers, anti-reflective lenses. • The wearing of corrective lenses is encouraged where they are required by staff members or pupils for DSE use. • Pupils should report to the class teacher if they experience any headaches or sore eyes, etc., as a result of DSE.	Y	Headteacher Office Manager	L
Orthopaedic injuries, such as repetitive strain		• Staff can adjust the height of their chairs and ensure they are arranged in such a way as to minimise the risks related	Y	Headteacher Office Manager	L

Potential risks	Risk rating prior to action H/M/L	Recommended controls	In place? Yes/No	By whom?	Risk rating following action H/M/L
injuries, caused by poor posture		to poor posture. • Staff and pupils are able to take 5 minute breaks from using digital technology every two hours to minimise the risks of orthopaedic injuries caused by sitting down or typing for long periods of time.			
Online grooming/radicalisation		• Pupils are termly advised on e-safety and the dangers of online grooming before using any school owned digital technology for the first time and at regular intervals thereafter. • Inappropriate websites, such as social-networking sites or extremist sites, where the dangers of online grooming or radicalisation are particularly high, are blocked or restricted using web-filtering software which is managed by the broadband provider. • Pupils' online activity is monitored by the teacher. • Pupils' behaviour is monitored by school staff for any signs of unusual behaviour which could indicate susceptibility to online grooming/radicalisation, e.g. change of dress, eating habits, etc. • Any unusual online activity or behaviour exhibited by a pupil is reported to the class teacher charge for further action, as per the school's Behavioural Policy and Online Safety Policy. • Pupils are also expected to report any concerns about their own online safety to their class teacher or supervising adult.	Y	DSL Headteacher Computing lead All staff	L

Potential risks	Risk rating prior to action H/M/L	Recommended controls	In place? Yes/No	By whom?	Risk rating following action H/M/L
Personal data is left unsecured/lost		• Computers, and other networked digital devices, are secured as per the school's Data Protection Policy. • Portable digital storage devices, such as flash drives or camera memory cards, memory sticks etc used by external companies/trainhers are to be encrypted. However, all portable devices are not to be used by staff or pupils in school. Staff and pupils are to use Sharepoint and Onedrive for data storage purposes. • All pupils have their own user account and their own password. This is managed internally by the computing lead and office manager securely.	Y	DSL Headteacher Office Manager Computing Lead All staff	L
The technology or any of its components, such as batteries, are not disposed of safely		• The least toxic and most reusable products, such as rechargeable batteries, are purchased where possible. • Obsolete or irreparable electronic equipment is returned to the retailer, or to a certified e-waste recycler or disposal service, for safe and proper disposal. • Toner cartridges, liquid and paste, as well as colour toner, are removed whole and intact to prevent the dispersal of toner, and then stored in suitable labelled containers prior to proper disposal by a certified e-waste disposal service. • Broken or unwanted hard drives are securely erased/degaussed and then physically destroyed by disk crusher, at a certified e-waste disposal service. • Batteries are never disposed of using fire.	Y	IT technician Office Manager	L

Potential risks	Risk rating prior to action H/M/L	Recommended controls	In place? Yes/No	By whom?	Risk rating following action H/M/L
Cyber attacks		• All digital technology networked at the school is secured in accordance with our Online Safety Policy. • Networked systems are secured with firewalls and clearly defined user privileges to prevent unauthorised access. • Anti-virus/malware software with heuristic threat analysis capability is procured where possible. • Anti-virus/malware checks run on every applicable piece of digital technology are maintained by the internet provider. • Anti-virus/malware software is maintained and updated by the internet service provider to ensure that it remains current to the latest cyber threats.	Y	IT technician	L