CRICKLADE MANOR PREP

E-Safety

Whole School	Reviewed	Next Review	Signed
Yes (including EYFS)	11/20	02/21	

STATEMENT FROM WISHFORD GROUP IT FUNCTION

We use BT Business Internet for our internet connection, and filter all internet requests through a Cisco Meraki firewall and content filtering device. All internet access requests using the School network (wired and wireless) go through this filter, which blocks access to websites in the following categories:

- Abused Drugs
- Adult and Pornography
- Alcohol and Tobacco
- Bot Nets
- Cheating (Academic)
- Confirmed SPAM Sources
- Cult and Occult
- Dating
- Gambling
- Gross
- Hacking
- Hate and Racism
- Illegal
- Keyloggers and Monitoring
- Malware Sites
- Marijuana
- Nudity
- Open HTTP Proxies
- Phishing and Other Frauds
- Proxy Avoidance and Anonymizers
- SPAM URLs
- Swimsuits and Intimate Apparel
- Unconfirmed SPAM Sources
- Violence
- Weapons

The websites covered by the categories above are updated automatically by Cisco Meraki from their global lists, to ensure up-to-date coverage. The Cisco Meraki system is maintained by the Wishford Group IT function.

Ian Harkess
Wishford Group IT Manager

E-SAFETY: POLICY GUIDANCE

Scope
This guidance is applicable to all those involved in the provision of e-based education/resources at the school and those with access to / are users of school ICT systems.

Objectives

1.1.1 To ensure that pupils are appropriately supervised during school activities.
1.1.2 To promote responsible behaviour with regard to e-based activities.
1.1.3 To take account of legislative guidance, in particular the General Data Protection Regulations and the Data Protection Act 2018.

Guidance

1.1.4 The DSL / Head Teacher will be responsible for the implementation of this policy.

1.1.5 The DSL will act as E- Safety Co-ordinator and will:

(a) compile logs of e-safety incidents;
(b) report to the Head Teacher on recorded incidents;
(c) ensure that staff are aware of this guidance;
(d) provide / arrange for staff training;
(e) liaise with school technical staff;
(f) liaise with the Head Teacher on any investigation and action in relation to e-incidents; and advise on e-safety policy review and development.

1.1.6 The Group IT Manager will:

(a) be responsible for the IT infrastructure and ensure that it is not open to misuse or malicious attack;
(b) ensure that users may only access the networks and devices through an enforced password protection policy;
(c) keep up to date with e-safety technical information in order to carry out their role;
(d) ensure that the use of the network (including internet, virtual learning, email and remote access) is monitored for misuse where deemed necessary; and
(e) implement any agreed monitoring software / systems.

1.1.7 Teaching and Support Staff will:

(a) maintain awareness of school e-safety policies and practices;
(b) report any suspected misuse or problem to the Head Teacher or E-Safety Co-ordinator;
(c) ensure that all digital communications with pupils / parents / carers/ fellow staff are on a professional level and conducted on school systems;
(d) where relevant e-safety is recognised in teaching activities and curriculum delivery;
(e) ensure pupils understand and follow e-safety policies, including the need to avoid plagiarism and uphold copyright regulations;
(f) monitor the use of digital technologies (including mobile devices, cameras etc during school activities); and
(g) ensure that where the use of the internet is pre-planned, pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
(i) Child Protection

Those responsible should be trained in e-safety issues and aware of the implications that may arise from:

(ii) sharing of personal data;
(iii) access to illegal / inappropriate materials;
(iv) inappropriate contact on-line with adults / strangers;
(v) potential or actual incidents of grooming; and
(vi) cyber-bullying.

Pupils

are responsible for using school digital technology systems in accordance with the Group acceptable use policy;

will understand and follow e-safety policies, including the need to avoid plagiarism and uphold copyright regulations;

will understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;

are expected to understand policies on the use of mobile devices and digital cameras, the taking / using of images and cyber-bullying; and will understand that the e-safety policy will include actions outside of school where related to school activities.

Parents / Carers

will be advised of e-safety policies through parents' evenings, newsletters, letters, school website etc;
will be encouraged to support the school in the promotion of good e-safety practice; and
should follow school guidelines on:
digital and video images taken at school events;
access to parents' sections of the school website / pupil records; and
their children's / pupils' personal devices in the school (where this is permitted).

1.1.8 Community Users / Contractors
1.1.9
Where such groups have access to school networks / devices, they will be expected to provide signed acceptance to abide by school e-safety policies and procedures.

Legal Requirements & Education Standards
References: A: Commentary on the Regulatory Requirements September 2018, Part 3 (www.isi.net) B: Reference Guide to the key standards in each type of social care service inspected by Ofsted (www.ofsted.gov.uk) C: Health and Safety at Work" Section H of the ISBA Model Staff Handbook D: "Health and Safety and Welfare at Work" Chapter N of the ISBA Bursar's Guide E: "Insurance" Chapter K of the Bursar's Guide by HSBC Insurance Brokers Ltd F: UK Council for Child Internet Safety (www.edcuation.gov.uk/ukccis) G: Cyber-bullying.org (www.cyberbullying.org) H: Department for Education "Safer Working Practice for Adults who Work with Children and Young People" (www.education.gov.uk) I: DfE Data Protection: a toolkit for schools

Risk Rating Matrix

The Risk Rating Matrix is a way of quantifying the risk associated with your activity. It works by using a simple multiplication table based around set levels of severity and likelihood, giving a result which is then graded using a traffic light system.

Both severity and likelihood are split into 5 categories, ranging from unlikely to certain for likelihood and minor injury to death for severity. Each category is given a value between 1 and 5, with 5 being the highest category and 1 the lowest. These values are used to work out the risk rating.

Risk Matrix – High – Medium – Low (Risk)						
Severity x Likelihood = Risk Rating		Likelihood				
		Certain (5)	Very Likely (4)	Likely (3)	May Happen (2)	Unlikely (1)
Severity	Death (5)	25	20	15	10	5
	Major Injury (4)	20	16	12	8	4
	Over 7 day injury (3)	15	12	9	6	3
	Minor Injury – treatment off site (2)	10	8	6	4	2
	Minor injury – first aid on site (1)	5	4	3	2	1

Severity x Likelihood = Risk Rating

The result of this will be between 1 and 25, which is then grouped into High, Medium or Low risk as below;

High Risk	**Medium Risk**	**Low Risk**
12 and above	between 11 and 5	4 and below

For each activity that you input on to the Risk Assessment, you will need to give it a Risk Rating. The form is designed so that it takes you through the multiplication; you are required to input severity, likelihood and the Risk Rating. If your activity comes out with too high a risk, that could be High or even Medium risks, there is space on the Risk Assessment to add more control measures and rate the risk again. This shows that you have adjusted the controls in reaction to the perceived risk.

Date of event:	Department:	Assessed by:	SBM Signature:	Risk Matrix – High – Medium – Low (Risk)
Ongoing	Whole School	J. Barton		Severity x Likelihood = Risk Rating

Severity	Likelihood: Certain (5)	Very Likely (4)	Likely (3)	May Happen (2)	Unlikely (1)
Depth (5)	25	20	15	10	5
Major Injury (4)	20	16	12	8	4
Over 7 day injury (3)	15	12	9	6	3
Minor Injury – treatment off site (2)	10	8	6	4	2
Minor injury – first aid on site (1)	5	4	3	2	1

Name of Event:	Type & Location of Event:	Description of Event:
E-safety	Whole of school and home	

Describe the hazard	Who might be harmed and how?	Existing control measures	Risk Rating Likelihood x Severity = RR			Additional control measures	Revised rating Likelihood x Severity = RR		
			L	S	RR		L	S	RR
Exposure to inappropriate online content Commercial – Adverts, Spam, Sponsorship, Personal info Extremist - Violent / hateful content Sexual - Pornographic or unwelcome sexual content Values– Bias, Racist, Misleading info or advice	Children / Staff	Appropriate Use Policy Appropriate filtering Reporting mechanism Children educated to report concerning images	2	5	10	Parent engagement through newsletter / parent portal Introduction of Be Internet Legend Assembly and supporting material Oct. 2020	1	5	5
Inappropriate online contact Commercial –Tracking, harvesting personal info Aggressive - Being bullied, harassed or stalked Sexual –	Children	Online Safety Policy Reporting mechanism Appropriate monitoring	2	5	10	Peer support programme Parental engagement programme	1	5	5

Meeting strangers, Being groomed Values– Self harm, unwelcome persuasions						Introduction of Be Internet Legend Assembly and supporting material Oct. 2020			
Inappropriate online behaviour Commercial –Illegal downloading, hacking, gambling, financial scams, terrorism Aggressive - Being bullied, or harassing others Sexual – Creating and uploading inappropriate material Values– Providing misleading info or advice	Children / Staff	Appropriate Use Policy Reporting mechanism Education programme Appropriate monitoring	2	5	10	Parental engagement programme Introduction of Be Internet Legend Assembly and supporting material Oct. 2020	1	5	5
Information and Data Security Data Protection – data loss or compromised Security Intrusion – information or access is compromised eg hack or virus/malware	Staff	Data Protection Policy Password policy GDPR Information Risk Officer	2	3	6	Regular reminder to staff regarding GDPR to lock screens. Ask all staff to sign updated Internet safety agreement Dec.2020	1	3	3
Online Safeguarding Staff capability to recognise, respond and resolve issues	Staff	Professional development programme including induction Professional support mechanism Senior leadership and Designated Safeguarding Lead responsibility	2	5	10	Be Internet Legends online course for teachers. Nov 2020 Review Induction to include internet safety training.	1	5	5