E-SAFETY RISK ASSESSMENT:

Date of Assessment: 21.1.2014

Updated: 17.3.2014, 27.11.2016, 3.5.2018, 6.11.2019, 29.3.2020, 5.6.2020, 4.10.2020, 23.5.2022, 27.11.2023

Assessed by: Kate Slatcher and Chelsie Nelmes

Section: Holymead Primary School **Review date: Sept 2024**

CONTENTS / Structure of Document:
IT H&S, Content, Contact, Conduct, Specific Application Risks, GDPR

Section 1 – IT access

What is the **Task/Activity** or **Environment** You Are Assessing?	What **Hazards** Are Present or May Be Generated?	Who is **affected** or **exposed** to hazards	What **Degree of Injury** Can Reasonably be Expected *(Risk Rating Matrix Table 1)?*	What **Precautions** are Already in Place to Either Eliminate or Reduce The Risk of an Accident Happening (**Existing Controls**)?	What **Likelihood/ Probability** is there of an Accident occurring? *(Risk Rating Matrix Table 1)?*	What is The **Risk Rating** *(See* Note *Below & Risk Rating Matrix Table 2)?*
Using computers, smartboards, PCs, net books, iPads	Physical issues e.g. repetitive strain injury, eye strain. theft.	Pupils, staff, volunteers, pupils	Serious	Follow H&S policies and procedures for using IT equipment, including interactive white boards e.g. not looking into bright projector lights. Take regular breaks from the computer, have appropriate furniture e.g. chairs at correct height. Follow school procedures for looking after assets e.g. lock away at night. Do not leave valuables lying around. See Display Screen Equipment / Office staff risk assessments.	Low	Low risk

E-SAFETY RISK ASSESSMENT:

What is the **Task/Activity** or **Environment** You Are Assessing?	What **Hazards** Are Present or May Be Generated?	Who is **affected** or **exposed** to hazards	What **Degree of Injury** Can Reasonably be Expected *(Risk Rating Matrix Table 1)?*	What **Precautions** are Already in Place to Either Eliminate or Reduce The Risk of an Accident Happening (**Existing Controls**)?	What **Likelihood/ Probability** is there of an Accident occurring? *(Risk Rating Matrix Table 1)?*	What is The **Risk Rating** *(See Note Below & Risk Rating Matrix Table 2*)?
Content						
Online searching. Downloading photos and information	Viewing unsuitable material. Downloading inappropriate material. Illegal downloads/ copyright infringement.	Pupils	Serious	1) School has firewall protection whereby unsuitable sites are blocked. 2) Pupils cannot download apps or access YouTube on devices which are managed through central system 3) Follow school Acceptable Usage of IT policy. Make parents aware of internet use by sending an internet agreement home for parents and pupils to read and sign. 4) Inform parents of possible dangers through the newsletter / email updates. 5) PSHE curriculum covers e-safety e.g. teaching pupils what to do if they find material they think is unsuitable, worrying. 6) Teach pupils to have an awareness of ownership of their own work and not to plagiarise. 7) Teach pupils to cross check websites to check the validity of information. 8) Reporting incidents to staff and recording in the incident book on site. Reporting searches that throw up indecent images. Keep in log book. 9) Staff initially mute sound or use blank screen to open online clips and disable auto play on YouTube to reduce the risk of inappropriate content or adverts seen / heard from interactive whiteboards	Medium	Medium risk

E-SAFETY RISK ASSESSMENT:

		Staff / Volunteers		1) New staff have to sign the E-safety policy to confirm they have read and understood the document. 2) Ensure GBM (technicians) set up new equipment with suitable safety protection / filtering via school wifi 3) Staff record any instances where inappropriate material can be accessed with IT leader / SLT / Incident log 4) Staff laptops can access You Tube – password protected access via device passcode 5) All online clips checked for content beforehand 6) Staff can investigate/monitor searches with Bristol IT, by recording dates and the IP address of the machine – Bristol can provide an emailed copy of all searches within time frames as required.		
		Device Security		iPads – connected to Wifi in school, IT leader updates iOS remotely to ensure latest security settings downloaded.		

E-SAFETY RISK ASSESSMENT:

What is the **Task/Activity** or **Environment** You Are Assessing?	What **Hazards** Are Present or May Be Generated?	Who is **affected** or **exposed** to hazards	What **Degree of Injury** Can Reasonably be Expected *(Risk Rating Matrix Table 1)?*	What **Precautions** are Already in Place to Either Eliminate or Reduce The Risk of an Accident Happening (**Existing Controls**)?	What **Likelihood/ Probability** is there of an Accident occurring? *(Risk Rating Matrix Table 1)?*	What is The **Risk Rating** *(See Note Below & Risk Rating Matrix Table 2)*?
Conduct						
Using mobile phones/ tablets/ i-pads	Bullying Grooming Sexting Taking inappropriate pictures Trolling Inappropriate use of internet searches	Pupils / Staff	Serious	PSHE curriculum covers e-safety eg teaching pupils what to do if they find material they think is unsuitable, worrying. Assemblies on contact with people we don’t know and the possible dangers and what to do ie tell a trusted adult. Follow mobile phone policy whereby phones/tablets are not allowed to be used in school by pupils. **Acceptable use policy** / Staff handbook signed by pupil and parents Record in incident books on site. Report to other agencies as necessary (follow e-safety flow chart for reporting).	Medium	Medium
Use of cameras on devices	Upskirting (KSCIE 2019/2020) Consent for photographs being breached Sexting Trolling	All	Serious	Pupils will use device cameras as part of their curriculum work. Pupils reminded about right to safe learning environment and will only take pictures if given verbal consent and only as part of curriculum work (see E-safety charters) E-Safety leader to monitor and delete photographs on iPads Pupil iPad are locked down so that social media cannot be accessed through the filtering system, thereby reducing risk of publication of any materials.	Low	Medium

E-SAFETY RISK ASSESSMENT:

				Class teachers ensure NO pupil takes inappropriate photographs NOTE that Keeping Children Safe in Education defines Up skirting and advises on Safeguarding procedures Staff and visitors to utilise school equipment to take photos both on and off site. No personal devices to be used Photograph permissions lists held in office. Teachers monitor that vulnerable children without permission e.g. Children in Care do not appear on events pages, or posts unintentionally (see Photo Permissions agreement)		
Misuse or unauthorised access to pupil accounts	Hacking pupil accounts (internally) Publishing false information on remote learning platform under different name	Pupils / Staff	Medium	As part of computing curriculum, pupils shown how to log out of devices and apps e.g. Google Classrooms and TTRockstars, to avoid accounts being accessed by other pupils. E-safety charter details not to share passwords with peers / friends Any breaches to be investigated by E-safety leader / Curriculum leads, pupil passwords changed on request from staff / parents Staff MUST use secure passwords. If compromised contact DSL, SLT, SBM to secure accounts immediately {Also see School system hacking / security below)	Low	Low
Use of school and personal		Staff / Governors/ Volunteers	Serious	Staff reminded regularly about **code of conduct/acceptable use** policies. Do not post anything that will bring themselves or the	Low	Medium

(BYOD) technology				school into disrepute**.** Avoid tagging individuals without their consent. Disciplinary action will be taken if there is inappropriate use of social media. Don’t use own phone/equipment with pupils. Don’t take photos of children on own phone – use a school iPad. Devices should be kept in drawers/bags with a secure passcode. Staff have access to mobile phones for emergencies during the day and on trips for keeping in touch with school. Volunteers need to be reminded not to use their devices on trips unless for approved/emergency use. Regular visitors/Holymead Hub users/staff have access to Holymead Guest Wifi (Bring Your Own Device) – This requires password and security certificate – emailed in advance/on arrival to site – this ensures correct filters are used in building. Staff discouraged from using 3G/4G/ 5G mobile data to bypass security settings within school e.g. to access social media. Staff and Visitors follow Mobile Phone policy in school, phones on silent, and if required only use devices in Holymead Hub, Staffroom or office spaces when pupils are not present in out of hours times.		

E-SAFETY RISK ASSESSMENT:

What is the **Task/Activity** or **Environment** You Are Assessing?	What **Hazards** Are Present or May Be Generated?	Who is **affected** or **exposed** to hazards	What **Degree of Injury** Can Reasonably be Expected *(Risk Rating Matrix Table 1)?*	What **Precautions** are Already in Place to Either Eliminate or Reduce The Risk of an Accident Happening (**Existing Controls**)?	What **Likelihood/ Probability** is there of an Accident occurring? *(Risk Rating Matrix Table 1)?*	What is The **Risk Rating** *(See Note Below & Risk Rating Matrix Table 2)?*
Contact						
Social networking and emailing. Gaming, X-boxes, Moshi Monsters, Snapchat, WhatsApp etc.	Contact with inappropriate people and material. Online bullying	Pupils	Serious	Follow safe- guarding policies and procedures. Links to PSHE and IT curriculum, Safer Internet Day. PSHE curriculum covers e-safety eg teaching pupils what to do if they find material they think is unsuitable, worrying. Teaching pupils how to keep safe eg not giving out phone numbers and addresses. Teaching pupils to realise the person they are talking to may not be the person they think they are eg adults posing as children. Inform parents of possible dangers by highlighting on newsletters. Make parents aware of cyber-bullying and sexting (and new technologies as they arise). Record in incident books on site. Report to other agencies as necessary (follow e-safety flow chart for reporting). Teaching pupils how to use ‘Comment’ features on forums on Google Classroom stream page and assignments in a monitored environment. Teaching pupils that what they put out online can affect others. Esafety leader gets information on latest threats from the UK Safer Internet Centre incorporates: SwGFL, Childnet International & Internet Watch Foundation.	Medium	Medium

E-SAFETY RISK ASSESSMENT:

What is the **Task/Activity** or **Environment** You Are Assessing?	What **Hazards** Are Present or May Be Generated?	Who is **affected** or **exposed** to hazards	What **Degree of Injury** Can Reasonably be Expected *(Risk Rating Matrix Table 1)?*	What **Precautions** are Already in Place to Either Eliminate or Reduce The Risk of an Accident Happening (**Existing Controls**)?	What **Likelihood/ Probability** is there of an Accident occurring? *(Risk Rating Matrix Table 1)?*	What is The **Risk Rating** *(See Note Below & Risk Rating Matrix Table 2*)?
Contact						
Emails / Social Media / Twitter	Inappropriate contact Phishing emails	Staff	Serious	Do not disclose personal or work email addresses. Direct all enquiries to office@holymeadprimary.co.uk Passwords changed regularly for laptops, email accounts, online services e.g. Google classrooms. Staff advised on secure passwords. All email communication to be professional in nature. Emails use secure filtering / Clutter filter. Ensure that you do not follow hyperlinks that then require further input of passwords. Email can be scanned / read by the school if suspicious activity is reported/suspected. Do NOT have pupils as friends on social media. Report any pupil friend requests to Head teacher – as pupils under 13, should not be using social media platforms. Staff living within the local community may have parents as friends, however staff reminded that everything they post, can reflect on them as an employee of the school – see code of conduct.	Medium	Medium

Specific Software / Application Risk Assessments

What is the **Task/Activity** or **Environment** You Are	What **Hazards** Are Present or May Be Generated?	Who is **affected** or **exposed** to hazards	What **Degree of Injury** Can Reasonably be Expected *(Risk Rating*	What **Precautions** are Already in Place to Either Eliminate or Reduce The Risk of an Accident Happening (**Existing Controls**)?	What **Likelihood/ Probability** is there of an Accident occurring? *(Risk Rating Matrix*	What is The **Risk Rating** *(See Note Below & Risk Rating Matrix*

E-SAFETY RISK ASSESSMENT:

Assessing?			Matrix Table 1)?		Table 1)?	Table 2)?
Use of Google Classroom for remote learning	Uploading content Posting comments Google Meet – video chat Youtube video links	Staff, pupils	Low / reputational damage	The option to send emails has been disabled – children will not be able to communicate with each other privately. When posting onto class stream, teachers must disable children's ability to comment when applicable. Staff to ensure documents being uploaded are appropriate and follow copyright laws . When using Google Meet - staff to be aware of when camera and microphone are switched off. Staff given training on how to hide Google meet code before scheduled meet – this assures staff will be first to sign in and then become the host. Each meet needs a new code to ensure all meets are closed effectively. Staff to conduct themselves following Code of Conduct, and consider surroundings if based at home are appropriate, and consider if headphones are used to maintain any confidential or sensitive information being shared if using a shared space, open classroom after school, or if meeting can be overheard from speakers. You Tube links should only allow children to view video attached – staff must report should this not be the case and cease from adding links. Information will then be passed onto Nigel to investigate and inform GBM support.	Low	Low
Use of SeeSaw for remote learning (active until Sept 22 for	Uploading content Posting comments as	Staff, pupils	Low / reputational damage	Contact: Pupils have individual secure logins with unique QR code and unique login text code. Pupils can only communicate directly with teacher, and all posts are reviewed and approved before being saved into individual pupil portfolio. No direct pupil to pupil content, unless enabled to class page, and teacher will approve all		

KS1)	audio, photo, video, file Youtube video links			posts in this instance. Family app not enabled – to manage security of account, and so that we don't manage security of family members commenting on work that would also need approval from a member of staff. Content: Teachers monitor quality / suitability of posts, and either delete or send back inappropriate post. In event of safeguarding concerns, screen shots taken and sent to Designated Safeguarding lead. Teachers monitor audio annotations by pupils and appropriate video content. Reference to the DSL if any safeguarding conerns. Holymead not responsible for external You Tube links, but will endeaviour to check external content is appropriate by watching the whole video – to check no inappripraite content half way through.. Conduct: Children to follow e-safety charter about suitable online behaviour e.g. use of photos, appropriate posts – any concerns, teacher to contact parent/carer in the first instance.		
Use of Zoom / Microsoft Teams	Inappropriate material shared online Reputational damage to school	Staff	Low / reputational damage	SEE SEPARATE ZOOM RISK ASSESSMENT and Pupil Charter If required, pre-recorded content e.g. videos, media, presentations with audio, can be published on the website. Zoom / Microsoft Teams managed by IT technicians, linked to professional school email address, and meetings booked by School Business Manager who is super user of the educational account. Staff to conduct themselves following Code of Conduct, and consider surroundings if based at home are appropriate, and consider if headphones are used to maintain any confidential or sensitive information being shared if using a shared space, open classroom after school, or if meeting can be overheard from speakers.	Low	Low

E-SAFETY RISK ASSESSMENT:

Use of Loom Software	Inappropriate material shared online Reputational damage to school	Staff / Pupils	Low	Turn off comments on Loom Turn off ability to download Staff to consider appropriate filming locations, clothing, conduct and content.	Low	Low
Use of social media videos to share pupil work.	Inappropriate material published by pupil Reputational damage to school	Pupil	Medium / reputational damage	School recognises some pupils are likely share video or multimedia content via You Tube or Vimeo, Facebook Holymead can host video content on the website, and also post links to external content (but accept no responsibility for this external content). Where possible we will host content on our year group pages to share with peers.	Low	Low

E-SAFETY RISK ASSESSMENT:

What is the **Task/Activity** or **Environment** You Are Assessing?	What **Hazards** Are Present or May Be Generated?	Who is **affected** or **exposed** to hazards	What **Degree of Injury** Can Reasonably be Expected *(Risk Rating Matrix Table 1)?*	What **Precautions** are Already in Place to Either Eliminate or Reduce The Risk of an Accident Happening (**Existing Controls**)?	What **Likelihood/ Probability** is there of an Accident occurring? *(Risk Rating Matrix Table 1)?*	What is The **Risk Rating** *(See Note Below & Risk Rating Matrix Table 2)?*
Online purchases	Misuse of school funds.	Staff	Serious Reputational damage	Follow school financial procedures in school policy. Delegation of duties in ordering, authorising and checking off deliveries. iTunes accounts for iPads NOT linked to the school credit card – top cards used as cash to prevent misuse / prevent accidental purchases. Staff request app purchases through subject leader / IT technician. Apple VPP payments processed by School Business Manager / Bursar.	Low	Low
School website School twitter accounts	Publishing inappropriate material. Data protection. Use of images.	Staff Pupils (particularly Looked After Children or vulnerable children)	Serious Reputational damage	Follow school's website policy including not naming children in images, checking pupils have completed acceptable use policy. Don't include any data or images covered by data protection rules/copyright. School Business Manager / SLT monitor posts on website. Colleagues within Year groups self-monitor each other for errors in grammar and spelling. Twitter Feeds/Website/Google Classroom/SeeSaw: Teaching staff are "Gatekeepers" that control and approve content for publication.	Low	Low

E-SAFETY RISK ASSESSMENT:

				"Super users" hold a central copy of access passwords / enhanced administration rights so that posts can be removed (including out of hours/holiday periods) – Head, Deputy heads, SLT, IT Leader, School Business Manager and Esafety Leader. Limited staff have enhanced access rights to remote learning platforms. Messages regarding school closures or Social Media / Press release approved by Head teacher only and communicated via ParentMail – not SeeSaw announcements or other social media channels..		
School systems being hacked remotely	Inappropriate material published by third party Data breach Website address hi-jacked to another site Online payment systems compromised resulting in financial loss or identify theft or card details lost to users of service	Staff	Serious	Use of secure platforms for websites that have up to date security measures. Limited number of users for websites, passwords regularly changed. Super users (see above) Third party companies are responsible for updating the security of their platforms e.g. external holders of parent data / payment methods. Third party responsible for systems secure from hacking attacks. Regular website monitoring and if hacking suspected or reported, report to website provider and close/suspend site. Use IT website systems that are paid services that protects as far as possible against hacking, and also have a point of contact for emergency out of hours support.	Low	Low

E-SAFETY RISK ASSESSMENT:

What is the **Task/Activity** or **Environment** You Are Assessing?	What **Hazards** Are Present or May Be Generated?	Who is **affected** or **exposed** to hazards	What **Degree of Injury** Can Reasonably be Expected *(Risk Rating Matrix Table 1)?*	What **Precautions** are Already in Place to Either Eliminate or Reduce The Risk of an Accident Happening (**Existing Controls**)?	What **Likelihood/ Probability** is there of an Accident occurring? *(Risk Rating Matrix Table 1)?*	What is The **Risk Rating** *(See Note Below & Risk Rating Matrix Table 2*)?
GDPR				**Privacy Notice Published on School website & school offices** **Protocols followed for access requests for information**		
Data breach	Personal data breach including financial information	All stakeholders	Low/Medium Reputational damage	Data Asset Register . Information Assest Register held – monitored by Data Controller / Governors. All third party suppliers must be GDPR compliant and recorded on Information Asset Register (IAR) Secure passwords used by all office staff for systems e.g. SIMS, ParentMail, after school club: staff should log out or lock computer. Data breach protocols followed by Data Processors who report to Data Controller (appointed Integra March 2018) – 72 hour reporting time is always applicable including school holidays and weekends. Autoreply set for “office email” and school answerphone stating that systems are not monitored.	Low	Low
Data storage	Loss / unauthorised access to pupil/staff/stake holder data	All stakeholders	Low/Medium Reputational damage	Secure systems provided by 3rd parties that are GDPR compliant e.g. SIMS, Target Tracker Monitor device use across Wifi network to check for unauthorised / Bring your own device (BOYD) items should be on Holymead Guest Wifi	Low	Low

E-SAFETY RISK ASSESSMENT:

				All laptops / iPads password/passcode protected Use of cameras only for trips (photos removed from SD card after trip and not kept on insecure data storage). Photos taken on iPads with a secure code. All staff NOT permitted to store pupil data on unencrypted memory sticks Sensitive paper documents: Staff should consider if they need to be printed. Shredder available to destroy near photocopier once documents no longer needed. Shredding reminders on display near photocopiers. Separate drives and different levels of access e,g, Pupil / Teachers / Admin / Management / Head – managed by IT contractor. Staff Performance Management Documents & Monitoring feedback are NOT to be saved on the central Teacher Drive – email to Head/Deputies and keep a copy in My Documents.		
Cloud Computing	Unauthorised access to sensitive pupil / staff data	Staff	Low / Reputational damage	2 factor authentication enabled on staff using Cloud technology (e.g. Google Drive that is GDPR compliant) Advise staff NOT to keep personal content in a work cloud Governor Hub used to share documentation – access set up via emails (School Business Manager/Clark monitor). Governor Hub GDPR compliant.	Low	Low
Medical Information	Pupil allergies / medication / sensitive information	Pupils with medical needs	Low/Medium	Parents made aware by letter that photographs of their child WILL be held on staffroom display board to ensure that staff are aware of any allergies and emergency medication.	Low	Low

	accessed			Parents/Carers made aware that this personal information may be seen by volunteers in the staffroom – the school consider this advantageous in the event of a medical emergency and not to the detriment of the child		
Religious dietary guidelines and restrictions	Discrimination	Individuals following religious dietary restrictions	Low/Medium	School office staff, kitchen staff and lunchtime supervisors aware of individual pupil's dietary requirements e.g. no pork, Halal – information stored in SIMS database and photos of pupils in kitchen areas	Low	Low
Remote access	Unauthorised access to sensitive pupil / staff data	All stakeholders	Medium / Reputational Damage	Secure remote access arrangements using GDPR compliant companies	Low	Low
Sending and sharing information	Unauthorised access to sensitive pupil / staff data	Staff: particularly Family Link Worker / SENCO / SLT	Medium / Reputational Damage	Communication with outside agencies should be via Holymead email and Bristol-schools.uk / official work email address. Do not send sensitive data by email unless authorised by Head/Designated Safeguarding Lead. All items kept in sent items box. Staff advised not to click REPLY ALL by mistake to emails	Low	Low
Awareness of GDPR	Failure to comply with new Data Protection Regulations	Staff / Governors	Medium / Reputational Damage	Work with Integra / Data Protection Officer to ensure compliance and identify best practice. Attend training / complete online training recommended by **Integra** or Trading with Schools/Governor Hub. Have GDPR as a standing item for Finance and Infrastructure Committee / FGB.	Low	Low
Data Breach	Unauthorised access to	Staff	Medium / Reputational	Microsoft Teams used to record details of call logs to parent/carers/families. Teachers to record dates and times of calls,	Low	Low

	sensitive pupil / staff data		Damage	and any concerns shared with Designated Safeguarding Lead using exisiting procedures / then CPOMs for SLT. Details of phone numbers have been sent to staff using Microsoft Email Accounts, with initials of pupils only. Staff advised not to print these lists and view on screen when in use. If using SIMS, staff to log out or lock screen if away from machine for any period of time to maintain security of this data.		

E-SAFETY RISK ASSESSMENT:

E-Safety Risk Assessment

Section 2 - ACTION PLAN

What is the **Hazard** You Need to Control ?	What **Additional Precautions** do You Need to Either Eliminate or Reduce the Risk to an acceptable level.	Who is **Responsible** For Implementing These Controls	**When** Are These Controls to be Implemented (Date)?	When **Were** These Controls Implemented (Date)?
Use of Google Classrooms	Discussion of the Risk Assessment for the specific application, and raising awareness of the 3Cs: Contact, Conduct and Content at the inset day.	Chelsie N	October 2020	October 2020
GDPR	Staff received GDPR leaflet from data controller to begin raising awareness of GDPR	School Business Manager / IT leads	May 2018	April 2018
Use of You Tube by pupils	Families received emails via Parent Mail about how they use You Tube, monitor pupil use. Staff advised to check that any You Tube or media is posted by the parent/carer, not the pupil.	Class teacher IT Leads E-safety leader	May 2020	May 2020
The school has a direct point of contact with these companies for technical support out of hours where possible: • Holymead website hosted by E-schools Ltd, 0845 557 8070, support@eschools.co.uk • Parent Mail: 01733 595962 / online contact form • Bristol City Council IT Services: 0117 90 37999, schools.it.helpdesk@bristol.gov.uk • Integra Carole Brown. GDPR@integra.co.uk / 01454 863950 • GBM (IT systems support): 07867 120 950 (Nigel Sluman), Office: 0161 605 3838 Bill Crocker: Delegated Services. M: 07795 190 130; bill.crocker@delegatedservices.org				

E-SAFETY RISK ASSESSMENT:

RISK RATING MATRIX

(Notes to aid completion of the risk assessment form)

Table 1

Potential Severity of Harm	Meaning	Likelihood of Harm	Meaning
Fatal/Major Injury	Death, major injuries or ill health causing long-term disability/absence from work.	High (Frequent)	Occurs repeatedly / event only to be expected
Serious Injury	Injuries or ill health causing short-term disability/absence from work (over three days absence)	Medium (Possible)	Moderate chance/could occur sometimes
Minor Injury	Injuries or ill health causing no significant long-term effects and no significant absence from work	Low (Unlikely)	Not likely to occur.

Table 2

Risk Rating - Degree of Injury by Likelihood/Probability			
	High (Likely)	**Medium (Possible)**	**Low (Improbable)**
Fatal/Major Injury	**Very High Risk**	**High Risk**	**Medium Risk**
Serious Injury	**High Risk**	**Medium Risk**	**Low Risk**
Minor Injury	**Medium Risk**	**Low Risk**	**No Significant Risk**

Table 3

Action Required : Key To Ranking	
High or Very High Risk	**STOP ACTIVITY!** Action MUST be taken as soon as possible to reduce the risks and before activity is allowed to continue.
Medium Risk	**Proceed with Caution!** Implement all additional precautions that are not unreasonably costly or troublesome.
Low Risk	**Proceed with Caution!** Implement any additional precautions that are not unreasonably costly or troublesome.
No Significant Risk	No further action required. The risk is no more than is to be encountered in normal every day life & is, therefore, regarded as being acceptable.