# E-SAFETY RISK ASSESSMENT:

**Date of Assessment: 21.1.14, updated 17.3.14, updated 27.11.16, 3.5.18** **Assessed by: Kate Slatcher and staff**
**Section: Holymead Primary School** **Review date: Sept 2018**

***Section 1***

| 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 eg repetitive strain injury,<br>Eye strain.<br>Theft. | Pupils, staff, volunteers, | Serious | Follow H&S policies and procedures for using IT equipment, including interactive white boards eg not looking into bright projector lights.<br>Take regular breaks from the computer, have appropriate furniture eg chairs at correct height.<br>Follow school procedures for looking after assets eg lock away at night. Don't leave valuables lying around.<br>See Display Screen Equipment / Office staff risk assessments. | Low | Low risk |

| 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** | | | | | | |
| On line searching. Downloading photos and information | Viewing unsuitable material.<br><br>Downloading inappropriate material.<br><br>Illegal downloads/ copyright infringement. | **Pupils** | Serious | 1) School has firewall protection whereby unsuitable sites are blocked. The school uses SWGFL as regional provider.<br>2) 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.<br>3) Inform parents of possible dangers through the newsletter / email updates.<br>4) PSHE curriculum covers e-safety eg teaching pupils what to do if they find material they think is unsuitable, worrying.<br>5) Teach pupils to have an awareness of ownership of their own work and not to plagiarise.<br>6) Teach pupils to cross check websites to check the validity of information.<br>7) Reporting incidents to staff and recording in the incident book on site. Reporting searches that throw up indecent images. Keep in log book. | Medium | Medium risk |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | **Staff / Volunteers** | | 1) New staff have to sign the Code of Practice for employees – see staff handbook<br>2) Ensure Vyssion (technicians) set up new equipment with suitable safety protection / filtering via school wifi<br>3) Staff record any instances where inappropriate material can be accessed with IT leader / SLT / Incidnet log<br>4) Staff laptops can access You Tube – password protected access via device passcode<br>5) All online clips checked for content beforehand<br>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** | | Kindles Not enabled on school wi-fi network to prevent purchase/viewing of unsuitable material.<br><br>iPads – connected to Wifi in school, IT leader updates iOS remotely to ensure latest security settings downloaded. | | |

| 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<br>Grooming<br>Sexting<br>Taking inapprorpiate pictures<br>Trolling<br>Inappropriate use of internet searches | Pupils | Serious | PSHE curriculum covers e-safety eg teaching pupils what to do if they find material they think is unsuitable, worrying.<br>Assemblies on contact with people we don't know and the possible dangers and what to do ie tell a trusted adult.<br>Follow mobile phone policy whereby phones/tablets are not allowed to be used in school by pupils.<br>**Acceptable use policy** / Staff handbook signed by pupil and parents<br>Record in incident books on site. Report to other agencies as necessary (follow e-safety flow chart for reporting). | Medium | Medium |
| | | Staff / Governors/ Volunteers | Serious | Staff reminded regularly about **code of conduct/acceptable use** policies. Do not post anything that will bring themselves or the school into disrepute**.** Avoid tagging individuals without their consent. Disciplinary action will be taken if there is inappropriate use of social media.<br>Don't use own phone/equipment with pupils.<br>Don't take photos of children on own phone – use a school iPad.<br>Devices should be kept in drawers/bags with a secure passcode<br>Staff have access to mobile phones for emergencies during the day and on trips for keeping in touch with school.<br>Volunteers need to be reminded not to use their devices on trips unless for approved/emergency use.<br>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.<br>Staff discouraged from using 3G/4G mobile data to bypass security settings within school. | | |

| 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.<br>Gaming, X-boxes, Moshi Monsters, Snapchat, WhatsApp etc. | Contact with inappropriate people and material.<br><br>Online bullying | Pupils | Serious | Follow safe- guarding policies and procedures.<br>Links to PSHE and IT curriculum, Safer Internet Day<br>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.<br>Teaching pupils to realise the person they are talking to may not be the person they think they are eg adults posing as children.<br>Inform parents of possible dangers by highlighting on newsletters. Make parents aware of cyber-bullying and sexting (and new technologies as they arise).<br>Record in incident books on site. Report to other agencies as necessary (follow e-safety flow chart for reporting).<br>Teaching pupils how to use email / 'Comment' fetures on forums on the blog website in a monitored environment. Teaching pupils that what they put out online can affect others.<br>Esafety leader gets information on latest threats from the UK Safer Internet Centre incorporates: SwGFL, Childnet International & Internet Watch Foundation. | Medium | Medium |

| 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<br><br>Phishing emails | Staff | Serious | Do not disclose personal or work email addresses. Direct all enquiries to office@holymeadprimary.co.uk<br>**Passwords changed regularly.**<br>All email communication to be professional in nature<br>Emails use secure filtering / Clutter filter. Ensure that you do not follow hyperlinks that then require further input of passwords.<br>Email can be scanned / read by the school if suspicious activity is reported/suspected.<br>**Blogging leader monitor use of Twitter** by staff to promote their blog.<br>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.<br>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 |

| 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<br>Reputational damage | Follow school financial procedures in school policy.<br>Delegation of duties in ordering, authorising and checking off deliveries.<br><br>iTunes accounts for iPads NOT linked to the school credit card – top cards used as cash to prevent misuse / prevent accidental pruchases. Staff request app purchases through subject leader / IT technician.<br><br>Apple VPP payments processed by School Business Manager / Bursar. | Low | Low |
| School website<br>School blog<br>School twitter accounts | Publishing inappropriate material.<br>Data protection.<br>Use of images. | Staff<br><br>Pupils (particularly Looked After Children or vulernable children) | Serious<br>Reputational damage | Follow school's website and blogging policy including not naming children in images, checking pupils have completed acceptable use policy.<br>Don't include any data or images covered by data protection rules/copyright.<br>School Business Manager / SLT monitor posts on website<br>Colleagues within Year groups self-monitor each other for errors in grammar and spelling.<br><br>Twitter Feeds/Website/Blog:<br>"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, IT Leader, Blog Leader, School Business Manager and Esafety Leader.<br><br>Limited staff have enhanced access rights to all blogs.<br>Messages regarding school closures or Social Media / Press release approved by Head teacher only. | Low | Low |
| School systems | Inappropriate | Staff | Serious | Use of secure platforms for websites that have up to date security | Low | Low |

| | | | | | | |
|---|---|---|---|---|---|---|
| being hacked remotely | material published by third party<br><br>Data breach<br><br>Website address hi-jacked to another site<br><br>Online payment systems compromised resulting in financial loss or identify theft or card details lost to users of service | | | measures.<br><br>Limited number of users for websites, passwords regularly changed. Super users (see above)<br><br>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.<br><br>Regular website monitoring and if hacking suspected or reported, report to website provider and close/suspend site.<br><br>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. | | |

| 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**<br><br>**Protocols followed for access requests for information** | | |
| Data breach | Personal data breach including financial information | All stakeholders | Low/Medium<br><br>Reputational damage | Data Asset Register . Information Assest Register held – monitored by Data Controller / Governors<br>All third party suppliers must be GDPR compliant and recorded on Information Asset Register (IAR)<br>Secure passwords used by all office staff for systems e.g. SIMS, ParentMail, after school club: staff should log out or lock computer.<br>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.<br>Autoreply set for "office email" and school answerphone stating that systems are not monitored. | Low | Low |
| Data storage | Loss / unauthorised access to pupil/staff/stakeholder data | All stakeholders | Low/Medium<br><br>Reputational damage | Secure systems provided by 3rd parties that are GDPR compliant e.g. SIMS, Target Tracker<br>Monitor device use across Wifi network to check for unauthorised / Bring your own device (BOYD) items should be on Holymead Guest Wifi<br>All laptops / iPads password/passcode protected<br>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.<br>All staff NOT permitted to store pupil data on unencrypted memory sticks<br>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 | Low | Low |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | photocopiers.<br>Separate drives and different levels of access e,g, Pupil / Teachers / Admin / Management / Head – managed by IT contractor<br>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)<br>Advise staff NOT to keep personal content in a work cloud<br><br>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 accessed | 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.<br>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 | Low | Low |
| 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 arrangments 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.<br>Do not send sensitive data by email unless authorised by Head/Designated Safeguarding Lead. All items kept in sent items box.<br>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.<br><br>Attend training / complete online training recommended by **Integra** or Trading with Schools/Governor Hub.<br><br>Have GDPR as a standing item for Finance and Infrastructure Committee / FGB. | Low | Low |

# 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)? |
|---|---|---|---|---|
| Inappropriate blog posts and moderating posts | -Teacher training on blog moderation<br>-Risk: photos attached to first names on home blog posts.<br>-Training for children about copyright free pictures / use for education purposes licencing using google filters<br>-Each teacher / year team has a Twitter account to promote blogging<br>-Staff Professional Identity – How we conduct ourselves and do not link personal accounts, opinions etc (Link to teaching standards and Code of Conduct for Employees) | Computing Leader<br>Computing Leader<br>Class teachers<br>Class teachers<br>E-safety leader | January 2017<br>December 2016<br>January 2017<br>March 2017<br>February 2017 | |
| GDPR | Staff received GDPR leaflet from data controller to begin raising awareness of GDPR | School Business Manager / IT leads | May 2018 | |

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
- Holymead Blog: hosted by Creative Blogs Ltd, Mill House, Hornby Road, Claughton, Lancashire, LA2 9LA Office: 01524 222099, Mobile: 07894 222671. support@creativeblogs.zendesk.com
  John Sutton & David Mitchell @deputymitchell deputymitchell@me.com
- Bristol City Council IT Services: 0117 90 37999, schools.it.helpdesk@bristol.gov.uk
- Integra Carole Brown
  GDPR@integra.co.uk / 01454 863950
- Vyssion 01249 454600
- Bill Crocker: Delegated Services. M: 07795 190 130; bill.crocker@delegatedservices.org

# 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. |