Risk Assessment Form

Risk Assessment Form - Part A

DEPARTMENT/ SERVICE	Telford Park School
Assessor/Person(s) assisting with the assessment	Tom Ward/ Paul Ray
TASK / ACTIVITY (Include duration and frequency of task activity)	**Whole site ICT hardware and systems – Risk Assessment of Online Safety and 4 C's**

Likelihood of Occurrence	**Severity of Outcome**				
	1 Negligible	2 Slight	3 Moderate	4 Severe	5 Very Severe
1 Very Unlikely	**LOW (1)**	**LOW (2)**	**LOW (3)**	**LOW (4)**	**LOW (5)**
2 Unlikely	**LOW (2)**	**LOW (4)**	**LOW (6)**	**MEDIUM (8)**	**MEDIUM 10)**
3 Possible	**LOW (3)**	**LOW (6)**	**MEDIUM (9)**	**HIGH (12)**	**HIGH (15)**
4	**LOW (4)**	**MEDIUM (8)**	**HIGH (12)**	**HIGH (16)**	**HIGH (20)**

Persons / groups at risk			
A	Employees	**E**	General Public / Pupils
B	New Employees	**F**	Visitors
C	Contractors / Sub-Contractors	**G**	Volunteers
D	Young person / Work experience	**H**	Clients / Service users

Online Safety – 4 C's Key Categories of Risk (also see TPA Online Safety Policy)	
Content	**Contact**
Conduct	**Commerce**

Probable 5 Very Likely	**LOW (5)**	**MEDIUM (10)**	**HIGH (15)**	**HIGH (20)**	**HIGH (25)**

Likelihood of occurrence X Severity of outcome = Risk Rating

Example: Likelihood (possible 3) X Severity (Moderate 3) = Risk Rating (Medium 9)

Risk Assessment Form - Part B

What are the hazards	Who might be harmed and how?	Online Safety - 4 Key Categories of Risk	What existing control measures are in place to reduce / prevent the risk?	Risk rating (refer to chart)	Further action required to eliminate or reduce the risk (who by and Date)	Residual risk rating (refer to chart)
Lack of parental consent and pupil ownership regarding use of hardware/software and online safety awareness	A, B, C, D, E	**Conduct**	Consent allows parents to make an informed decision about whether to allow their child to participate. It is also, an outward signal to parents that we take online safety seriously. This forms part of the pupil transition form. Pupil code of conduct also forms agreement between school and pupil around use of technology. Code of conduct posted on website under appendix a of the school behaviour policy. All pupils must also agree to our ICT systems acceptable use agreement on start-up of their device – failure to do so denies access to device/system.	3	Parental engagement and awareness raised by DSL. Publication and review of online safety policy.	3

What are the hazards	Who might be harmed and how?	Online Safety - 4 Key Categories of Risk	What existing control measures are in place to reduce / prevent the risk?	Risk rating (refer to chart)	Further action required to eliminate or reduce the risk (who by and Date)	Residual risk rating (refer to chart)
Education awareness raising around online safety and use of hardware/software	A, B, C, D, E, F, G, H	**Content, Contact, Conduct, Commerce**	Curriculum delivery in place as per page 7 of the online safety policy. Understanding the integral part that this plays in the curriculum, with additional sessions led by the school DSL at key intervals during the year. In the event of an incident, restorative conversations and return from FTE (where appropriate) meetings take place to educate individual and ensure that the incident does not reoccur.	4	Curriculum delivery reviewed and implemented by DSL with use of external providers where necessary to enhance provision.	4
Moderation of online use to detect potential child abuse or improper use of ICT systems	A, B, C, D, E, F, G, H	**Content, Contact, Conduct, Commerce**	Moderation in place via online classroom monitoring solution, 'Senso'. Improper use, 'trigger words' alert key members of the safeguarding team and temporarily block user devices/pages dependent on severity until the action is dealt with. Filtering system 'Smoothwall' in place to ensure that websites and content which breach school policy are not permitted. Access tailored to pupil/staff members dependent on role with high level of security enforced.	3	Periodic reviews of the Senso structure. Patterns analysed by the safeguarding team and used to inform discussion. Smoothwall and Senso developments discussed with ICT provider periodically.	3
Unauthorised access to staff/pupil accounts	A, B, C, D, E, F, G, H	**Contact, Commerce**	Fine-grain password policy in place which ensures that all accounts are reset on a 90-day cycle. All passwords must be complex in nature.	5	Developments discussed with managed service	5

What are the hazards	Who might be harmed and how?	Online Safety - 4 Key Categories of Risk	What existing control measures are in place to reduce / prevent the risk?	Risk rating (refer to chart)	Further action required to eliminate or reduce the risk (who by and Date)	Residual risk rating (refer to chart)
			Microsoft multi-factor authentication used on all staff devices, restricting the possibility of a data-breach. Microsoft Bitlocker encryption in place on all devices – meaning that if a devices is stolen/found, the device cannot be accessed by anyone but the school ICT Manager. Fully encrypted cloud-based server solution not stored on site at school premises, managed via Telford & Wrekin ICT services with daily backups. Staff/pupil leaver accounts managed by ICT Manager and system 'Salamander' which syncs daily to the MIS to ensure that accounts are up to date and only members of the organisation can gain access.		provider periodically to further enhance security based on market availability.	
Training of staff to reduce the risk of ensure integrity of school network.	A, B, D, E	**Contact, Content**	All staff complete NCSC Cyber Security and GDPR for education training annually as a minimum. All staff read and understand the online safety policy and understand what to do in the event of a safeguarding or online safety concern.	4	Updates circulated to all staff as necessary via trust/managed service/DFE/NCSC.	4
Virus/Malware/Phishing attack on school network	A, B, C, D, E, F, G, H	**Contact, Content**	Antivirus protection is installed on all machines and updates every 2	5	Updates circulated to all staff as necessary	5

What are the hazards	Who might be harmed and how?	Online Safety - 4 Key Categories of Risk	What existing control measures are in place to reduce / prevent the risk?	Risk rating (refer to chart)	Further action required to eliminate or reduce the risk (who by and Date)	Residual risk rating (refer to chart)
			hours. Any portable media is scanned when attached though school policy blocks all unauthorised devices unless pre-approved by ICT Manager. All incidents of phishing reported via the ICT Manager on occurrence. Regular updates from TAW ICT and ICT manager on avoidance of scam emails. Internal vulnerability assessments carried out by TAW on a weekly basis to assess integrity of network. Restrictions in place to ensure that only ICT Manager can authorise software downloads.		via trust/managed service/DFE/NCSC.	

Name of Assessor	**Tom Ward/ Paul Ray**	**Signature**	*T.Ward*

Name of Manager responsible for activity / process	**Tom Ward/ Paul Ray**	**Signature**	*T.Ward*

Risk Assessment Form - Part C

Links to other risk assessments and or safe working instructions - please state	Anti-bullying policy, Behaviour policy (inclusive of pupil code of conduct, appendix a), CAT privacy notices, Child on child abuse policy, Child protection and safeguarding policy (plus appendix 1), Complaints policy, Data protection policy, ICT and internet acceptable use agreement, PSHE and RSE policy, TPA Online Safety Policy, Risk assessment policy, Staff code of conduct, CEOP, KCSIE, Teaching Online Safety in Schools	
Name and Sign **When the assessment is complete it should be signed to say that is the case and all identified actions have been implemented.**	Tom Ward	**Originally Published** 23/12/2023

Review - Before work starts, it is important to consider the content on this risk assessment to ensure it is still valid.

For example, are there any significant changes, additions or omissions at the site not identified on the assessment? Are there any additional hazards or risks?

Please record any changes required and or action taken, then date and sign.

Reviewer Name & Date	Tom Ward 15/03/2023	**Notes**	Reviewed with SLT
Reviewer Name & Date	Tom Ward 12/05/2023	**Notes**	Reviewed with STW Telford & Wrekin Safeguarding Board
Reviewer Name & Date	EAB	**Notes**	Presented at EAB 15/05/2023
Reviewer Name & Date		**Notes**	

Monitoring and Review

Re-assessment will be completed every two years or sooner if there have been significant changes in example methods of working or equipment or a change of location.

Successful monitoring and review relies on commitment from managers at all levels and should therefore be included as an integral part of business planning process.

Sources of Further Information

HSE Risk Assessment: a brief guide to controlling risks in the workplace:

http://www.cleapss.org.uk/

http://www.afpe.org.uk/