Juniper Hill School – Risk Assessment and Cyber Response Plan
Cyber Security reviewed January 2026

YesPurpose of Risk Assessment	**People Involved**
We rely on technology and the internet to run Juniper Hill School and educate the children. Cyber attacks are a very real threat. The challenge all organisations have is the cyber threat landscape is complex and constantly changing. This risk assessment has been written to identify possible cyber threats and how they would impact the smooth running of the school and disrupt the children's learning. We have identified what we have put in place to protect ourselves from a cyber attack and what additional measures are necessary. It is important to make staff aware that Cyber Security is NOT an IT issue. It's an issue for all users and needs to be on the Juniper Risk Register. The school needs to include Cyber Security on the Emergency Response Plan and Business Continuity Plan. It is vital that Juniper keeps up to date with the latest security patches, updates and software. The school has a clear strategic plan around depreciation - end of security support = end of life.	ALL members of the Juniper Community

ACTION: School Risk Protection Arrangement (RPA) members to meet the cyber cover conditions

To ensure your school is covered for cyber incidents you must meet the following four conditions:

1. have off-site backups **We have this at Juniper with TurnItOn**
2. all employees or governors who have access to the member's information technology system must undertake National Cyber Security Centre training **All staff have received National Cyber Security Centre Training. Ask Luisa Davis to make sure any new staff are registered for the training. All staff complete monthly Boxphishing training**
3. register with Police CyberAlarm **Debbie Hill to register Juniper.**
4. have a cyber response plan in place – **Juniper's cyber response plan is at the end of the risk assessment.**

Theme What are the hazards?	**Who might be harmed and how? (Who is at special risk)**	**What are you already doing? (Current control measures, including those for people at special risk)**	**What further action is necessary? (Further control measures)**	**RISK LEVEL (Low, Medium, High)**	**Action by whom**	**Additional Information/ Review Notes.**

1) **Malicious Software**	Potentially all of the school computers and server could be infected. All staff could be impacted, the malware could be used to secretly gather data and send information to a third party.	As spam and phishing emails are the primary way in which malware infects computers, we need to make sure our email system is locked down tight. All Staff have received cyber security training and have been told to check attached documents carefully before they open them.	Share with the staff tips for recognising a malware email. • Sender's email address. ... • Email subject or attachment contains username. ... • Enticement to open an attachment. ... • Enticement to follow a link. ... • Information verification. ... • Problem warning, threat, or urgency. ... • Undisclosed-recipients/unlisted-recipients. ... • Suspicious attachment. Provide staff with regular cyber security training.	Medium The staff need to be aware of the risk at all times.	All members of the Juniper Team	Debbie Hill (IT Manager) to work with turnITon to make sure Trend Micro has the latest updates installed. To implement any recommendations from turnITon.
2) **Ransomware**	All members of the Juniper Team. The staff could be denied access to the school files on their computers.	The school has set up off site backups with turnITon The school uses a filtering system to only allow file types it would expect to receive. The filtering system blocks websites that are known to be malicious. This prevents users from accessing portions of the internet.	All staff complete monthly Boxphish training. (Cyber Security Awareness Training Platform)	Low	All members of the Juniper Team	NB staff can use the website ScamAdviser to check the safety and legitimacy of a website.

		The school devices are centrally managed in order to permit applications trusted by the school to run on the devices.				
3) **Loss of systems**	All members of the Juniper Team. The staff could be denied access to the school files on their computers.	The school has off site remote backups, to protect against human error and power outages. The school has a UPS battery that will power up if the system goes down. The staff aren't allowed to use memory sticks, this is written into all job-based risk assessments. The school works with turnITon to ensure we are using the most up to date antivirus software. Staff have been informed they are not to leave laptops in their cars or other transportation vehicles unattended. The staff know they need to be careful when powering down their computer, they must shut off any programs first.	We need to budget for a rolling programme of replacement devices. Ask the staff to dust their laptops regularly. Debbie Hill to make sure all mobile devices in school are maintained and regularly dusted. Ask the staff not to drink whilst using their laptops. Spillages can cause internal damage, coffee can pose a particular risk as it can corrode the inside of a computer.	Low	All members of the Juniper Team	We have a clear data destruction policy, this has been shared with staff, staff have been asked to follow the policy.

		Most documents are now stored on OneDrive / SharePoint.				
4) **Denial of service attack**	All members of the Juniper Team. The staff could be denied access to the school files on their computers.	The staff have been told to lock their laptops when they aren't using them / in the classroom teaching – this will ensure network endpoints (desktops, laptops etc) do not become an entry point for malicious activity. We are currently using Trend Micro, which gives us complete user protection, including antivirus, antispam, web security, ransomware protection and data security.		Low DoS attacks are often targeted towards high-profile organisations.	All members of the Juniper Team	We have a data destruction policy, this has been shared with staff, staff have been asked to follow the policy.
5) **Data Breach / Theft**	All members of the Juniper Team.	In general, data breaches happen due to weaknesses in technology and user behaviour. The staff have been told about the importance of having strong passwords and not sharing their passwords. Staff know they mustn't write passwords down and leave them in school.	We need to budget for a rolling programme of replacement devices. We need to make sure we upgrade all devices when any software is no longer supported by the manufacturer and always use the latest web browser. Make sure staff know that security is only as strong as the weakest link! Every person that interacts with a	Medium	All members of the Juniper Team	Debbie Hill to check access rights for all staff and maintain an access rights register. All staff are completing Boxphish monthly training.

		The staff have been told to lock their laptops when they aren't using them / in the classroom teaching. We keep a list of all staff that use the VPN. Once a staff member leaves Juniper they are removed from the system and can no longer access the school system / emails etc. The school doesn't allow shared accounts. Debbie Hill and turnITon regularly monitor what is happening on the school system.	system can be a potential vulnerability! We need to make sure that staff only have access to the systems / areas of the network they need.			
6) **Pupil Threats**	The children and all members of the Juniper Team.	We teach the children about passwords, privacy settings, protecting their identity and location as part of our unit of learning on Internet Safety and Harms. Our weekly newsletter shares online safety tips with our families, e.g., monitoring your child's activities online, utilising parent controls etc.	Phising marks the start of over 90% of modern cyber-attacks. We need to make sure as part of our online safety lessons we teach the children about cyber security, they need to be careful about what they click on and the games they download.	Medium	The Juniper Community, (families, children and staff).	Look at updating the Internet Safety and Harms unit of learning / adding additional lessons in Y5 / Y6.

			We also need to teach the children about identity fraud and protecting their data online as they grow up.			
7) **Fraud / Financial Losses**	All members of the Juniper Team.	The office staff have been trained as part of their cyber security training not to share any school financial details, not to click on any emails asking for payment they don't recognise etc.	Share what is Take Five website to support all members of the Juniper Community https://www.takefive-stopfraud.org.uk/	Low risk for Juniper Hill School, possibly medium / high risk for individuals.	All members of the Juniper Community	We can create a culture where we share resources we find / educate the adults to prevent them becoming victims of fraud.
8) **Insider Threats**	All members of the Juniper Team.	Once a staff member leaves Juniper they are removed from the system and can no longer access the school system / emails (emails are disabled) etc. The staff complete regular GDPR training. Staff lock their laptops when not in use / they leave their classrooms. All data is backed up remotely and on site.	We need to make sure cyber security continues to be part of our continuing CPD. Add a statement about Cyber Security / Insider Threats to the Staff Code of Conduct. The Staff Code of Conduct is signed annually as part of the performance management cycle.	Low	The Juniper Team	
9) **Unauthorised Data Changes**	All members of the Juniper Team.	Inform the staff that unauthorised data change is professional misconduct and a criminal offence.	Add a statement about Cyber Security / Unauthorised Data Changes to the Staff Code of Conduct. The Staff Code of Conduct is signed annually	Low	The Juniper Team	

			as part of the performance management cycle.			

Glossary

Term	Meaning
A Data Breach	A data breach exposes confidential, sensitive, or protected information to an unauthorized person. The files in a data breach are viewed and/or shared without permission. Anyone can be at risk of a data breach — from individuals to high-level enterprises and governments
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Denial-of-Service (DoS) attack	An attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software which uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Insider Threats	Threats posed by individuals from within an organisation, such as current or former employees, contractors and partners
Loss of Systems	A system failure is a problem either with hardware (other than disk) or with operating system software that causes your system to end abnormally

Malicious Software	Malicious Software is any product that intends to harm a PC, server or nay network, e.g. worm, virus or trojan.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (like bank details) or encouraging them to visit a fake website.
Ransomware	Ransomware is malware designed to deny a user or organisation access to files on their computer. By encrypting these files and demanding a ransom payment for the decryption key, this places organisations in a position where paying the ransom is the easiest and cheapest way to regain access to their files.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spam	Irrelevant or unsolicited messages sent over the internet, typically to a large number of users, for the purposes of advertising, phishing, spreading malware, etc.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A program that cannot reproduce itself but masquerades as something the user wants and tricks them into activating it so it can do its damage and spread.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virtual Private Network (VPN)	An encrypted network which allows remote users to connect securely.
Virus	Programs designed to self-replicate and infect legitimate software programs or systems.
Worm	A standalone piece of malicious software that reproduces itself and spreads from computer to computer.

Juniper Hill School – Cyber Security Response Plan

- **Recognise / Act / Isolate** - Staff member to turn off the machine instantly, hold down the power button. **DO NOT TURN THE MACHINE BACK ON**
- **Alert** – Inform Debbie Hill (IT manager) in her absence, Claire Garnett (Headteacher)
- **Detect** – Debbie Hill to find the issue / Debbie to log the incident with TurnItOn (01865) 597620 or NCSC https://report.ncsc.gov.uk/ 0300 1232040
- **Investigate** – TIO to work with the school to investigate
- **Treat** – TIO
- **Monitor** – TIO to support the school after the attack
- **Report** – Claire Garnett to report incident to DPO (Data Protection Officer) The school uses TurnItOn.