E security King's Oak Primary School

2017/2018

Signed by Chair of Governors: Paul Davies Dated: September 2017

Signed by Head teacher: A.J. England Dated: September 2017

Reviewed September 2017
Approved by FGB September 2017
Next review due September 2019

E security King's Oak Primary School

E security policy/best practice concerns all data created, modified, accessed, passed on or retained by staff on devices in or outside of school.

Appendix 1 – updated annually by IT Manager to measure integrity of systems in school.

USB Sticks/flash drives/portable hard drives:

1. Sensitive/confidential data should only be saved on school PCs within school.
2. Transfer of that data should only be done using encrypted flash drives/external hard drives.
3. All pupil/staff data accessed within school should be treated as confidential. If printed copies are made, they must be shredded at the end of use.
4. Printed copies of confidential data should **not** be taken out of or created outside of school.

Passwords:

Staff passwords must be kept private. Only the holder can change them. IT staff can help reset passwords but do not know what they are. Integris passwords are administered by the Business Manager.

General school computer, laptop, tablet and other IT device usage:

- School information systems may not be used for private purposes.
- Images should not be googled in front of the class. Ensure appropriate images are checked and saved before a lesson.
- Internet access is intended for school related purposes e.g. learning resources, educational websites, researching curriculum topics, use of email on school business and Integris.
- Remember confidentiality and do not disclose information from the network, divulge passwords or leave a PC unattended when logged in.
- If your smartboard is on, it displays whatever is on your monitor. This might include email, confidential documents, or school registers. You must always be aware whether it is appropriate for pupils, parents or visitors to see this. When away from your desktop you should lock your computer. (start+L)
- Use electronic communications in an appropriate way that does not breach the Data Protection Act 1998. (GDP regulations from May 2018).
- Do not provide your login details for cover usage. There are specific supply and visitor logins available to access the network.
- Staff should keep any data which is held on their school laptop to a minimum.
- Pupil specific IPads should not be taken off the school premises at any point.
- IPads should be returned to their cabinet for security/charging at the end of each school day.
- IPads allocated to specific members of staff should not be taken off site.

Email usage:

- School email should **ONLY** be used for ~~al~~l school matters and CHECKED regularly
- DO NOT pass on your King's Oak Primary email or your personal email address to parents. Invite parents to use the following email address **enquiries@kingsoakprimary.co.uk** for any form of electronic communication
- Sensitive/confidential data MUST NOT be sent by email unless the files are password protected.
- Emails should not be printed unless absolutely necessary and then shredded after use.
- Email retention - All King's Oak Primary email is retained for a minimum 5 years.

Staff's personal social media accounts:

- Ensure that content posted on any social networking, blogging or messaging service (including text or images) does not damage the reputation of the school or cause concern over their suitability to work with children.
- Ensure that issues relating to children or staff are not discussed on these networks.
- Be aware that if content posted is considered inappropriate, staff could render themselves vulnerable to criticism or allegations of misconduct.
- You should set your account security/privacy on networking sites to 'high'.

Use of Personal Devices and Mobile Phones:

- Phones must not be connected through the school network physically or wirelessly.
- Do not use mobile phones to take pictures, video or record audio of any pupil or staff member.
- Do not use your mobile around the school site without prior authorisation by the Headteacher.

Backups:

The school maintains regular nightly scheduled backups of all network data, both on and offsite (encrypted). This is held for a minimum of 5 years.
Pupil personal Information cards are kept in paper form and locked away securely in the event of no internet access/emergency
Paper Registers for all classes are kept in the event of no internet access/emergency

Door access cards:

Should only be used by the person named on the card. Visitors and temporary staff access cards are logged to named persons as they are issued. All access records are retained for a minimum of 5 years.

Internal telephone system:

School phones should only be used for school business. Do not give the school number or an internal direct dial number as a contact for non-school business. Telephone logs are retained for a minimum of 5 years.

CCTV:

The school has an extensive CCTV installation for the security and safety of all staff and pupils. All video is retained for approx. 30 days on a rolling basis. Any specific incident is retained for a minimum of 5 years.

APPENDIX 1

	Critical Security Control	Questions for School network Managers & Technicians	Questions for School Headteachers, Senior Leaders and Governors	Done in house	Done by Broadband service provider	Done by another service provider
1.	**Inventory of Authorised and Unauthorised devices:** Actively manage (inventory, track and correct) all hardware devices on the network so that only authorised devices are given access and unauthorised and unmanaged devices are found and prevented from gaining access	• Do you have a detailed up to date list of all network hardware and devices on your network? • Do you have processes in place to regularly review and update this? • Do you have the mechanisms and /or processes in place to detect when/if any unauthorised devices are connected to your network and to prevent any such devices from gaining access to data and facilities?	• Does your school's IT acceptable use policy (AUP) include provisions/instructions to ensure only authorised devices are connected to the school's network?			
2.	**Inventory of Authorised and Unauthorised software** Actively manage (inventory, track and correct) all software on the network so that only authorised software is installed and can execute and that unauthorised and unmanaged software is found and prevented from installation or execution.	• Do you have a detailed, up to date list of software used in school? • Do you have processes in place to regularly review and update this as necessary? • Do you have the mechanisms and/or processes in place to detect when/if any unauthorised software is installed on the network and to further prevent any such software from being used?	• Does your school's IT acceptable policy (AUP) include provisions/instructions to ensure only authorised software is used in school?			
3.	**Secure configurations for hardware and software on mobile devices, laptops, workstations and servers** Establish, implement and actively manage (track, report on, correct) the security configuration of laptops, servers and workstations using a rigorous configuration of management and change control processes in order to prevent attackers from exploiting vulnerable services and settings.	• Do you have standard secure configurations for the operating systems and applications used in school, together with processes to ensure these are consistently applied and maintained for example, re-imaging with secure builds if any system becomes compromised? • Do you have patching tools and processes update hardware and software promptly? • Are administrative privileges appropriately allocated and limited? • Do you have details of the lifecycles of all your software and hardware – do you know when manufacturers' support for hardware and software will end and what will you do when it does?	• Does your school's IT acceptable use policy (AUP) include clear provisions/instructions warning users about tampering with secure configurations with clear sanctions for any infraction? • Do you have visibility of likely costs to upgrade and refresh hardware and software as necessary and when these costs are likely to be incurred (for example antivirus software subscriptions, firewall support and maintenance services, dates for when hardware/software will go 'end of life' and need to be replaced)?			

4.	**Continuous vulnerability assessment and remediation** Continuously acquire, assess and take action on new information in order to identify vulnerabilities, remediate and minimize the window of opportunity for attackers	• How do you ensure you keep abreast of new and emerging risks and issues, reviewing and updating your e-security processes, software and hardware accordingly? • How do you ensure updates and patches are applied in a timely fashion once vulnerabilities have been identified?	• Do you have processes in place for regular review of e-security functions and your IT acceptable use policies top address new and emerging threats? • How do you ensure staff and pupils receive appropriate e-security advice and training?			
5.	**Malware defences** Control the installation, spread and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defence, data gathering and corrective action.	• How do you prevent malware across your school's network? • How regularly do you check that no malware is present? • How do you ensure that anti-malware software is kept up to date? • What steps do you take to ensure that malware risks from removable media like USB flash drives are minimised?	• How do you ensure that your user education processes and IT acceptable use policies are up to date to minimise risks in this area? • What sanctions are applied for malicious use of school IT services and systems?			
6.	**Application software security** Manage the security lifecycle of all in house developed and acquired software in order to prevent, detect and correct security weaknesses	• How do you ensure that you are using the most up to date versions of software? • Do you know when manufacturer support for the software you are currently using will end? What will you do when it does? • What e-security track record does the vendor of any new software you are considering have?	• Do you have visibility of when significant upgrade and renewal software will be required, both in terms of likely cost and ensuring service continuity? • How do you ensure staff and pupils are trained in the use of new software?			
7.	**Wireless Access control** The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (LANS), access points and wireless client systems.	• How do you ensure only authorised devices can connect to your school's wireless network? • How do you manage and maintain security for devices which are used both in and away from school? (for example, staff laptops and/or pupil owned devices if a bring your own device policy is in place – how to access provided to untrusted devices, if this is required)? • How do you ensure services and systems are kept secure if guest access of BYOD options are provided?	• What is the school's policy on wireless access – do you allow guest access, or access from staff or pupil owned devices? • Does your IT AUP appropriately encompass access from staff or pupil-owned devices if this is allowed? • Do your staff and pupils understand their obligations and responsibilities in relation to using their own devices in school, if they are allowed to do so?			
8.	**Data recovery capability** The processes and tools used to back up critical information properly with a proven methodology for timely recovery	• Do you have process in place for backing up school data securely and restoring it in the event of a security incident? • How regularly are backups made? • Where are the backups stored and how secure are your storage arrangements? • How quickly could you restore critical school data from a backup if you needed to do so?	• Does your school have an overarching disaster recover/business continuity plan? • If so, does this encompass restoration of IT facilities and critical school data appropriately?			

9.	**Security skills assessment and appropriate training to fill gaps** For all functional roles in the organisation (prioritising those mission – critical to the business and its security), identify the specific knowledge, skills and abilities needed to support defence of the enterprise; develop and execute an integrated plan to assess, identify gaps and remediate through policy, organisational planning, training and awareness programmes.	• Do you have an understanding of the skills, abilities and training needs of all members of your team? • How do you keep up to date with new and emerging security threats?	• Does your school's overarching staff training and development planning include provisions to ensure that technical support staff can keep up to date with e-security risks and best practices and that all teaching and administrative personnel understand their own e-security obligations and responsibilities?			
10.	**Secure configurations for network devices such as firewalls, routers and switches** Establish, implement and actively manage (track, report on, correct) the security configuration of the network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.	• Do you have policies and processes for ensuring and maintain secure configurations for all network devices such as firewalls, routers and switches? • How do you securely manage and implement any necessary changes to these devices and ensure they are kept up to date? • If support is provided by a third party, how do you maintain security if the third party if the third party were to discontinue its services for any reason?	• Do you have visibility/awareness of when major changes and /or upgrades will need to be carried out, in terms of both likely cost / budgeting and maintain service continuity?			
11.	**Limitation and control of network ports, protocols and services** Manage (track/control/correct) the ongoing operational use of ports, protocols and services on networked devices in order to minimise windows f vulnerability available to attackers.	• How do you ensure that only the necessary ports, protocols and services are running on each system? • How do you manage and maintain your firewall(s) to ensure it/they is/ are secure, up to date and supporting the needs of the school?	• Do you have visibility of when major changes are likely to be necessary? • Do you have effective processes for communicating changes, for example in relation to changing security settings to allow access to a new service or facility – are appropriate risk assessment and management processes in place and adhered to?			
12.	**Controlled use of administrative privileges** The processes and tools used to track/control/prevent/correct the use, assignment and configuration of administrative privileges on computers, networks and applications.	• How do you ensure administrative privileges are allocated appropriately? • Do you have complex password requirements for all administrator accounts? • How do you ensure that all default passwords are changed?	• Do you have effective user education strategies in place to ensure the importance of administrator privileges are understood and respected? • Does you IT acceptable use policy require strong, complex passwords and regular password changes?			

13.	**Boundary defence** Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.	• Are your boundary defences multi-layered? (for example encompassing firewalls, proxies, DMZ perimeter networks, network based intrusion detection and prevention) • Do you maintain any blacklists of known malicious sites or white lists of trusted sites? • How do you provide secure remote access to your network, if required?	• How regularly are your boundary defences reviewed and tested? • Do you employ any independent third party testing of your boundary defences to maintain their effectiveness in the light of dynamic and emerging threats?			
14.	**Maintenance, monitoring and analysis of audit logs** Collect, manage and analyse audit logs of events that could help detect, understand or recover from an attack	• Do you keep and review sufficient log information to be able to detect, recover and learn from a security incident? • How do you ensure you have sufficient storage arrangements for monitoring and logging data, for example to provide evidence in relation to an as yet undiscovered security incident?	• How do you ensure that sufficient time is allocated to reviewing and acting upon the outputs from monitoring and logging activities? • Where do responsibilities for reviewing outputs from monitoring and logging reside? • What are your data retention policies and where are they described?			
15.	**Controlled access based on the need to know** The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g. information, resources systems) according to the formal determination of which persons, computers and applications have a need and right to access these critical assets based on an approved classification.	• How do you differentiate access by user group (staff, pupils, IT support personnel)? • How do you limit access to services and sensitive data on your network only to authorised users?	• Does your IT acceptable use policy differentiate between the obligations and responsibilities of different groups of users (teaching staff, administrative/managerial staff, pupils, Governors)? • How do you communicate with and keep different user groups up to date with their obligations an responsibilities?			
16.	**Account monitoring and control** Actively manage the life cycle of system and application accounts – their creation, use dormancy, deletion – in order to minimise opportunities for attackers to leverage them.	• What processes are employed for provisioning, managing, monitoring and deleting user accounts as required? • How often is the list of current user accounts reviewed? • Do you employ an expiration date for inactive/dormant accounts? • As users required to lock screens when leaving devices temporarily unattended? • Is a strong password policy requiring regular new passwords in place and enforced? • Do you undertake any monitoring of user accounts for unusual usage?	• How do you communicate with, educate and inform different user groups of their obligations and responsibilities? • How regularly is your IT AUP updated in the light of new threats and lessons learned from previous incidents?			

17.	**Data Protection** The processes and tools used to prevent data exfiltration, mitigate the effects of ex-filtrated data and ensure the privacy and integrity of sensitive information (ex-filtration, the unauthorised release of data from within a computer system or network).	• Do you encrypt all sensitive data? • Do you know where all your schools' data is held – in school, in private clouds, the public cloud? • For data held in the cloud, do you have a strategy for switching cloud provider if required, or for ensuring that all your schools' data can be extracted from the service if required? • Do you have processes and policies in place to prevent theft or loss of devices – for example, can sensitive data be written to encrypted USB flash drives for removal from school premises?	• Are all staff an pupils aware of their responsibilities and obligations in relation to sensitive and personal data, particularly in light of schools' roles as data controllers under the Data Protection Act 1998?			
18.	**Incident response and management** Protect the organisation's information, as well as the reputation, by developing and implementing an incident response infrastructure (e.g. plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence and restoring the integrity of the network and systems.	• Do have defined processes for responding to and managing security incidents? • Are the roles and duties of key individuals sufficiently defined to ensure effective action is taken quickly in the event of a security incident? • Are logs and records kept for all incidents?	• How regularly are incident handling processes reviewed? • Do you undertake any example incident scenarios to test and update incident handling processes and procedures?			
19.	**Secure Network engineering** Make security an inherent attribute of the enterprise by specifying, designing and building in features that allow high confidence systems operations while denying or minimising opportunities for attackers.	• How regularly do you review your whole network infrastructure, polices, procedures in the light of new security technologies and techniques and emerging risks and issues? • How easy is it to make changes to update and improve security protections? • Do you employ any third parties to review your infrastructure, policies and procedures and suggest improvements?	• How much and how often are time and resources allocated to reviewing and updating the school network as a whole? • What processes and analysis are employed to determine which security functions are best provided in house which should be delivered using the expertise of third parties such as broadband service providers?			
20.	**Penetration tests and red team exercises** Test the overall strength of an organisations defences (the technology, the processes and the people) by stimulating the objectives and actions of an attacker	• Do you conduct any internal or external penetration testing of your schools' network? • How do you respond and learn from the results from such exercises?	• How do you identify sources of advice and support that can scrutinise the security of your network and suggest an action plan for improvement?			

IT Manager: …… Signed: ……

Date: ……..

Review Date: ……