2017

Online safety policy

A Ogle
Alderman Peel High School, Wells Primary and Nursery School, Burnham Market Primary School
Date: 30th January 2017

Table of Contents

Writing and reviewing the Online Safety policy

This policy is part of the School's Statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection processes.

- Ofsted inspectors will always make a written judgement under leadership and management about whether or not the arrangements for safeguarding children and learners are effective.
- The school will identify a member of staff who has an overview of Online Safety, this would usually be the Designated Safeguarding Lead (DSL).
- Our Online Safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by senior leadership and approved by governors.
- The Online Safety Policy and its implementation will be reviewed annually
- It was approved by the Governors: October 2016
- Date of next review: October 2017

Guidance and Example documents (separate documents):

- Legal Framework
- Example Pupil ICT Code of conduct
- Example Staff, Governor, Visitor ICT Code of conduct
- Example Parental/Carer Permission: Use of digital images – photography and video
- Example Parent/Carer ICT Code of Conduct agreement form (Feb 2016)
- Guidance for schools: Parents & Carers use of photography and filming at school events
- Guidance on the use of CCTV in schools including the Use of Fixed Video Cameras in the Classroom

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community with respect to the use of technologies.
- Safeguard and protect the children and staff.
- Assist school staff working with children to work safely and responsibly with technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of technologies for educational, personal or recreational use for the whole school community.

- Have clear structures to deal with online abuse such as online bullying [noting that these need to be cross referenced with other school policies].
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows:

Content

- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

Conduct

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)

Scope

This policy applies to all members of our schools community (including staff, students/ pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school technologies, both in and outside of our schools.

Communication

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website
- Policy to be part of school induction pack for new staff, including information and guidance where appropriate

- Regular updates and training on online safety for all staff, including any revisions to the policy
- ICT Code of Conduct to be issued to whole school community, on entry to the school.
- Handling Concerns
- The school will take all reasonable precautions to ensure online safety is in line with current guidance from the Department for Education (DfE)
- Staff and pupils are given information about infringements in use and possible sanctions.
- Designated Safeguarding Lead (DSL) acts as first point of contact for any safeguarding incident whether involving technologies or not
- Any concern about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the concern is referred to the Chair of Governors

Review and Monitoring

The online safety policy is referenced within other school policies (e.g. Safeguarding and Child Protection policy, Anti-Bullying policy, PSHE, Computing policy).

- The online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- There is widespread ownership of the policy and it has been agreed by the Senior Leadership Team (SLT) and approved by Governors. All amendments to the school online safety policy will be disseminated to all members of staff and pupils.

Education and Curriculum

Pupil online safety curriculum

This school:

- has a clear, progressive online safety education programme as part of the Computing curriculum/PSHE and other curriculum areas as relevant. This covers a range of skills and behaviours appropriate to their age and experience
- will remind students about their responsibilities through the pupil ICT Code of Conduct
- ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright
- ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/ intellectual property rights

Staff and governor training

This school:

- makes regular up to date training available to staff on online safety issues and the school's online safety education program
- provides, as part of the induction process, all staff [including those on university/ college placement and work experience] with information and guidance on the Online Safety Policy

Parent/Carer awareness and training

This school:

- provides information for parents/carers for online safety on the school website
- parents/carers are issued with up to date guidance

Incident management

In this school:

- there is strict monitoring and application of the online safety policy, including the ICT Code of Conduct and a differentiated and appropriate range of sanctions
- support is actively sought from other agencies as needed (i.e. the local authority, UK Safer Internet Centre helpline, CEOP, Police, Internet Watch Foundation) in dealing with online safety issues
- monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school
- parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible
- the Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law
- we will immediately refer any suspected illegal material to the appropriate authorities – i.e. Police, Internet Watch Foundation and inform the LA

Managing IT and Communication System

Internet access, security and filtering

In this school:

We follow guidelines issued by the Department for Education to ensure that we comply with minimum requirements for filtered broadband provision

Critical Security Control

Questions for School Head Teachers, Senior Leaders and Governors

1. Inventory of Authorized and Unauthorized Devices: Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

Does your school's ICT Code of Conduct/acceptable use policy (AUP) include provisions/ instructions to ensure only authorised devices are connected to the school's network?

2. Inventory of Authorized and Unauthorized Software: Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

Does your school's ICT Code of Conduct/acceptable use policy (AUP) include provisions/ instructions to ensure only authorised devices are connected to the school's network?

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 management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

Does your school's ICT Code of Conduct/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.

Do you have processes in place for regular review of e-security functions and your IT acceptable use policies to 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 ensure that your ICT Code of Conduct/acceptable use policy (AUP) 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. Do you have visibility of when significant upgrade and renewal of 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. What is the school's policy on wireless access – do you allow guest access, or access from staff- or pupil-owned devices?

Does your ICT Code of Conduct/acceptable use policy (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.

Does your school have an overarching disaster recovery/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 organization (prioritizing 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, organizational planning, training, and awareness programs.

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 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 visibility/awareness of when major changes and/or upgrades will need to be carried out, in terms of both likely cost/budgeting and maintaining 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 minimize windows of vulnerability available to attackers.

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.

Do you have effective strategies in place to ensure the importance of administrator privileges are understood and respected?

Does your ICT Code of Conduct/acceptable use policy (AUP) 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.

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.

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.

Does your ICT Code of Conduct/acceptable use policy (AUP) 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 and responsibilities?

16. Account Monitoring and Control: Actively manage the life-cycle of system and application accounts – their creation, use, dormancy, deletion – in order to minimize opportunities for attackers to leverage them.

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?

17. Data Protection: The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of

sensitive information (exfiltration: the unauthorized release of data from within a computer system or network)

Are all staff and pupils aware of all their responsibilities and obligations in relation to sensitive and personal data, particularly in the light of schools' roles as data controllers under The Data Protection Act 1998?

18. Incident Response and Management: Protect the organization's information, as well as its 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.

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 minimizing opportunities for attackers.

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 and 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 organization's defences (the technology, the processes, and the people) by simulating the objectives and actions of an attacker

How do you identify sources of advice and support that can scrutinise the security of you network and suggest an action plan for improvement?

E-mail

This school

- Provides staff with an email account for their professional use, e.g. nsix.org.uk and makes clear personal email should be through a separate account
- We use anonymous e-mail addresses, for example head@, office@
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date

Pupils email:

- We use school provisioned pupil email accounts that can be audited

- Pupils are taught about the online safety and 'netiquette' of using e-mail both in school and at home.

Staff email:

- Staff will use LA or school provisioned e-mail systems for professional purposes
- Access in school to external personal e mail accounts may be blocked

School website

- The school web site complies with statutory DfE requirements
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;

Social networking

Staff, Volunteers and Contractors

- Staff are instructed to always keep professional and private communication separate.
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.
- The use of any school approved social networking will adhere to ICT Code of Conduct

Pupils:

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- Students are required to sign and follow our [age appropriate] pupil ICT Code of Conduct.

Parents/Carers:

- Parents/carers are reminded about social networking risks and protocols

Data Security

Management Information System access and data transfer

- Please use guidance from the Information Commissioner's Office to ensure that you comply with your responsibilities to information rights in school

Equipment and Digital Content

Bring Your Own Device Guidance for Staff and Pupils

- Not allowed

Digital images and video

In this school:

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school (or annually)
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs
- Staff receive the school's ICT Code of Conduct and this includes a clause on the use of personal mobile phones/personal equipment
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term, high profile use

Author	Alastair Ogle
Ratification Date	
Review Date	
Signed Chair of Governors	
Date	