Online Safety Policy

Online Safety Policy

Introduction

This topic may be referred to as Online Safety or e-safety throughout this policy.

What is an Online Safety Policy?

- The school OnlineSafety policy aims to create an environment where pupils, staff, parents, governors and the wider school community work together to inform each other of ways to use the internet responsibly, safely and positively.
- Internet technology helps pupils learn creatively and effectively and encourages collaborative learning and the sharing of good practice amongst all school stakeholders. The Online Safety policy encourages appropriate and safe conduct and behaviour when achieving this.
- Pupils, staff and all other users of school related technologies will work together to agree standards and expectations relating to usage in order to promote and ensure good behaviour.
- These agreements and their implementation will promote positive behaviour which can transfer directly into each pupil's adult life and prepare them for experiences and expectations in the workplace. It is intended that the positive effects of the policy will be seen online and offline; in school and at home; and ultimately beyond school and into the workplace.

Ofsted context:

Ofsted have defined e-safety thus (in their previous 'Inspecting e-safety in schools' briefings):

- 'In the context of an inspection, e-safety may be described as the school's ability to protect and educate pupils and staff in their use of technology and to have the appropriate mechanisms to intervene and support any incident where appropriate.'

E-safety will be inspected in relation to the following areas:

- 'The behaviour and safety of pupils at the school.
- The quality of leadership in, and management of, the school'

Ofsted have identified three areas of e-safety risk in relation to pupils:

- 'Being exposed to illegal, inappropriate or harmful material.
- Being subjected to harmful online interaction with other users.
- Personal online behaviour that increases the likelihood of, or causes, harm.'

Online Safety Policy

1. Aims and Objectives
    - School internet use will be designed for pupil use and include filtering that is appropriate to the age of the pupils.
    - Pupils will be taught what internet use is acceptable and they will be given clear guidelines for its use. (Pupils agree to an Acceptable Use policy when they log on to the school network)
    - Pupils will be educated in the effective use of the internet for research; including location, retrieval and evaluation.
    - The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law.
    - Pupils will be taught the importance of cross-checking information, before accepting its accuracy
    - Pupils will be taught how to report unpleasant internet content e.g. using the CEOP report abuse icon or Hector protector

2. Managing Internet Access

    2.1 Information System Security
    - School ICT system security will be reviewed regularly.
    - Virus protection will be reviewed regularly.
    - Security strategies will be discussed with the local authority.

    2.2 Email
    - Pupils may only use approved school email accounts.
    - Pupils must tell a member of staff immediately, if they receive an offensive email.
    - In email communication, pupils must not reveal their personal details, or those of others, or arrange to meet anyone.
    - Incoming emails should be treated with suspicion and attachments should only be opened if the author is known.
    - Emails from pupils to external bodies will be supervised and monitored by an adult.
    - The forwarding of chain letters is not permitted.

    2.3 Published content and the school website.
    - Staff or pupil personal contact information will not be published. The contact details given online will be that of the school office or of staff emails.
    - The head teacher will take overall editorial responsibility and ensure content is accurate and appropriate.

    2.4 Publishing pupil's images and work.
    - Photographs that include pupils will be selected carefully, so that images cannot be misused.
    - Pupil's full names will not be used anywhere on the school website, particularly in association with photographs.
    - Written permission from parents or guardians will be obtained before photographs of pupils are published on the school website.
    - Pupil image file names will not refer to the pupil by name.
    - Parents will be clearly informed of the school policy on photographs.

    2.5 Social Networking and Personal Publishing
    - Social networking sites will not be accessed through the school network.
    - Children will be educated on the dangers of social networking sites, their age restrictions and how, when approariate to use them safely.

- Pupils will be advised never to give out personal details of any kind that may identify them, their friends or location.
- Pupils and parents will be advised that use of the social networking sites brings a range of dangers to primary age pupils.
- Pupils will be advised to use nicknames or avatars, if using social networking sites (when age aprropriate).

2.6 Managing Filtering

- The school network operates a filtering system, managed by Trustnet
- The school will work with Trustnet (London Grid for Learning) to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the online safety co-ordinator/ Network Manager and/or the safeguarding lead.
- SMT will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

2.7 Managing Emerging Technologies

- Emerging technologies will be assessed for their benefits and for any potential risks.
- Mobile phone use will not be allowed in school when children are present (see mobile phone use policy).
- If children bring a mobile phone to school for safety when travelling home (Year 6) they will be stored in the front office during the school day.
- Visitors and new staff are made aware of the mobile phone policy when signing in.

3. Policy decisions

3.1 Authorising Internet Access

- Parents will sign and return safety an internet agreement as part of the home/school agreement.
- Lessons involving internet access will include a specific online safety element.
- Children will be directed to appropriate sites, where possible, and internet access will only be under adult supervision.

3.2 Assessing Risks

- The school will take reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of the internet, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school or Sandwell LA can accept liability for any material accessed.
- The school will monitor online safety and check that the policy is relevant and implementation is appropriate and effective.

3.3 Handling online safety complaints

- Complaints of internet misuse will be dealt with by SMT
- Any complaint about staff misuse must be referred to the headteacher.
- Complaints of a safeguarding nature must be dealt with in accordance with the school's safeguarding procedures.
- Clear and transparent procedures exist for monitoring, logging, reporting incidents, evaluating, improving and measuring the impact of e-safety. All staff, parents, pupils, contractors and governors know how to report an online safety incident.

4. Introducing Online Safety to pupils
    - Online safety rules will be on display in rooms where computers are used
    - The home/school agreement will include online safety rules
    - Online safety training will be delivered through computing lessons, PSHE, assemblies, Safer Internet week and online training.
    - Online safety provision is always designed to encourage positive behaviour and practical real world strategies for all members of the school and wider school community.
    - Online safety will be covered as a computing unit and in other units children will learn how to judge the validity of websites and other aspects of computer usage.
    - Online safety will also be taught through PSHE e.g. how to deal with cyber bullying, how to report cyber bullying, and the social effects of spending too much time online.
    - Online safety events will take place – such as 'Safer Internet' week and 'Anti-Bullying Week'.
    - Pupils will agree to an Acceptable Use policy when they use the computer and are required to use school internet and computer systems in agreement with the terms specified in the school Acceptable Use policy.
    - Pupils will be informed that the network and internet use will be monitored and appropriately followed up.
    - Pupils need to be aware of how to report online safety incidents in school, and how to use external reporting facilities, such as the CEOP report abuse button.
    - Pupils need to be aware that the school Acceptable Use policy covers all computer, internet and gadget usage in school.
    - Pupils need to be aware that their internet use out of school on social networking sites is covered under the Acceptable Use policy if it impacts on the school and/or it's staff and pupils in terms of cyber bullying, reputation or illegal activities.

5. Staff and Online Safety
    - All staff understand online safety issues and that online safety is a school priority.
    - Teachers and teaching support staff will ensure that they are aware of the current school online safety policy, practices and associated procedures for reporting online safety incidents
    - School senior management is responsible for determining, evaluating and reviewing online safety policies to encompass teaching and learning, use of school IT equipment and facilities by pupils, staff and visitors, and agreed criteria for acceptable use by pupils, school staff and governors.
    - The school is working towards an e-safety Mark.
    - Training in online safety is provided to all staff.
    - All staff will read and accept the online safety policy.
    - Staff will include online safety in planning their Computing lessons.
    - Staff will be made aware of the importance of monitoring network and internet use.
    - Staff will use child friendly searches on the internet and teach children about trustworthy internet sites.
    - The Network Manager and the apprentices/ technicians are responsible for maintaining the school's networking, IT infrastructure and hardware. They need to be aware of current thinking and trends in IT security and ensure that the school system, particularly file-sharing and access to the Internet is secure. They need to further ensure that all reasonable steps have been taken to ensure that systems are not open to abuse or unauthorized external access, with particular regard to external logins and wireless networking.

- Support staff also need to maintain and enforce the school's password policy and monitor and maintain the internet filtering.
- All staff need to ensure that they are mindful when using social media, in regard to external off site use, personal use (mindful of not bringing the school into disrepute), possible contractual obligations, and conduct on internet school messaging or communication platforms, for example email, forums and the school website (see the staff handbook).
- All teaching staff need to rigorously monitor pupil internet and computer usage in line with the policy. This also includes the use of personal technology such as cameras, tablets and other gadgets on the school site.
- Teaching staff should promote best practice regarding avoiding copyright infringement and plagiarism.
- Internet usage and suggested websites should be pre-vetted and documented in lesson planning
- Staff must be aware of their responsibilities under the General Data Protection Regulation of May 2018 and ensure that personal and sensitive data is securely processed. Any such data sent electronically should be encrypted (See the Data Protection policy). All staff should use encrypted storage systems (memory sticks) if they must store sensitive data. If possible these details are to remain on the school system and not be transferred.

6. Online Safety Roles and Responsibility

6.1 Online Safety Co-ordinator: Jo Donnelly
Network Manager: Michael Oakes
Designated Safeguarding Person (DSP): Wendy Richmond
Head Teacher: Sally Baker
Governors: The Provisions Committee

6.2 Co-ordinating Online Safety

- The school has a designated Online Safety Co-ordinator [Under role of Computing Co-ordinator] who works with the Designated Safeguarding Person (DSP) and reports to the SLT and Governors and co-ordinates online safety provision across the school and wider school community.
- The school Online Safety co-ordinator is responsible for online safety issues on a day to day basis and also liaises with LA contacts, filtering and website providers and school ICT support.
- The school Online Safety co-ordinator audits and assesses INSET requirements for staff, support staff and governor online safety training, and ensures that all staff are aware of their responsibilities and the school's online safety procedures. The co-ordinator is also the first port of call for staff requiring advice on online safety matters.
- Although all staff are responsible for upholding the school online safety policy and safer internet practice, the Online Safety co-ordinator, the Designated Safeguarding Person (DSP) and ICT support are responsible for monitoring internet usage by pupils and staff, and on school machines, such as laptops, used off-site.
- The network manager will always take into account the needs of the users – i.e. the pupils and teachers. It is the responsibility of the network manager to implement online safety effectively without restricting or altering the requirements of the users.

- The network manager will carry out regular audits and evaluations of the school IT network and should maintain an ongoing development plan for IT provision.
- Servers, network switches, hubs, Cat5 or Fibre Optic cabling, wireless transmitters, bridges, access points and other physical architecture should be secured to prevent unauthorised or untraceable network access.
- The DSP will differentiate which online safety incidents are required to be reported to CEOP, local Police, LADO, social services and parents/guardians; and also determine whether the information from such an incident should be restricted to nominated members of the leadership team.

6.2 Governor's responsibility for online safety

- The Governors provisions committee will be responsible for online safety to coincide with their safeguarding responsibility.
- The school Online Safety co-ordinator will liaise directly with the provisions committee with regard to reports on online safety effectiveness, incidents, monitoring, evaluation and developing and maintaining links with local stakeholders and the wider school community.

7. Enlisting parents and carers support
    - Parents will sign the home/school agreement which contain the online safety rules.
    - Parents' and carers' will be aware of online safety through workshops, website information, newsletters and online safety activities.
    - It is expected that parents and guardians will support the school's stance on promoting good internet behaviour and responsible use of IT equipment both at school and at home.
    - The school expects parents and guardians to sign the home/school agreement, indicating agreement regarding their child's use and also their own use with regard to parental access to school systems such as extranets, websites, forums and social media.
    - The school will provide opportunities to educate parents with regard to online safety.

8. Policies to be used alongside the Online Safety Policy
    - Safeguarding Policy
    - Keeping Children Safe in Education
    - Computing policy
    - Anti- Bullying Policy
    - PSHE &C Policy

9. Policy Review Schedule
    - This policy was approved by governors and staff and is stored on the school network and is published for parents and the wider community on the school website.
    - The Online Safety policy will be monitored annually.
    - The Online Safety policy will be reviewed and evaluated in light of online safety incidents or changes in legislation.

Online Safety Policy

Date agreed: February 2018

Date to be reviewed: September 2020