Online Safety

Policy Date: Sum 2017
Review Date: Aut 2018

This policy applies to all members of the school (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school IT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other Online Safety incidents covered by this policy, which may take place outside of the school but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school.

Education – Pupils

- A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and lessons.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.

Education – Parents / Carers

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site
- Parents / Carers evenings / sessions/ online courses
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications

Education & Training – Staff / Volunteers

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.
- The Online Safety Coordinator will receive regular updates through attendance at external training events (eg from CEOP/ LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff or team meetings / INSET days.
- The Online Safety Coordinator will provide advice / guidance / training to individuals as required.

Governors should take part in online safety training / awareness sessions.

Technical – infrastructure / equipment, filtering and monitoring

School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.

- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and password. Users are responsible for the security of their username and password.
- Internet access is filtered for all users
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Mobile Technologies

The school Acceptable Use Agreements for staff, pupils/students and parents/carers states the appropriate use of mobile technologies.

Use of digital and video images

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website / social media / local press.
- In accordance with guidance from the Information Commissioner's

Office, parents / carers are welcome to take videos and digital images of their children at school / academy events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.

- Pupils must not take, use, share, publish or distribute images of others without their permission
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupil's work can only be published with the permission of the student / pupil and parents or carers.

Data Protection

The school will ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy (see appendix for template policy)
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)

Staff will ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and

other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.

- Transfer data using encryption and secure password protected devices or the data must be encrypted and password protected
- The device used for transferring the data has virus and malware checking software
- The transferred data must be deleted from any device, in line with school policy once it has been transferred or its use is complete.

Communications

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students / pupils or parents / carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content.
- Pupils at KS2 and above will be provided with individual school email addresses for educational use.
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.

School staff ensure that:

- No reference is be made in social media to students / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Monitoring of Public Social Media
- Monitor the Internet for public postings about the school

The school's use of social media for professional purposes will be checked regularly by the Headteacher and Online Safety Coordinator to ensure compliance with the school policies.

Websites for Reference

https://www.internetmatters.org/ has a wealth of guidance for all working with children and is strongly supported by many national organisations.

"Supporting School Staff" is an essential document to help staff understand how to protect themselves online created by Childnet 5 International and DfE: http://www.digizen.org/resources/schoolstaff.aspx

The National Safer Internet Centre's Professional Online Safety

https://www.ceop.police.uk/safetycentre/ offers advice and guidance around e-Safety for professionals who work with children and young people in the UK. It is also to be used for reporting any unlawful or threatening behaviour online. The helpline provides support with all aspects of digital and online issues such as social networking sites, cyber-bullying, texting, online gaming and child protection online. Staff can contact the helpline via 0844 381 4772, mailto:helpline@saferinternet.org.uk or can visit www.saferinternet.org.uk/helpline for more information.

"Guidance for Safer Working Practice for Adults who Work with Children and Young People" (2009) contains useful guidance around professional use of technology. www.childrenengland.org.uk/upload/Guidance%20.pdf

Schools have a duty of care to safeguard and protect staff under the Health and Safety at Work Act 1974 and the Management of Health and Safety at Work Regulations 1999. Key legislation also includes Section 11 of the Children Act 2004 which places a duty on key persons and bodies to ensure that their functions are discharged having regard to the need to safeguard and promote the welfare of children. Schools may also wish to read and consider the document

"Guidance for Safer Working Practice for Adults who Work with Children and Young People" (2009), which contains useful guidance around professional use of technology.
www.childrenengland.org.uk/upload/Guidance%20.pdf