Sir John Cass's Foundation Primary School

Safe use of digital resources

Date adopted	5th July, 2017		Notes
Last Reviewed	8/5/18		School Policy
Review Cycle	As necessary		
Review by	Headteacher		

1. **Context**
    a. Our aim is to ensure that children are seen, heard and helped in the contexts of their lives both online and offline.
    b. With the growing use of technology and social media, all professionals need to adopt a much more sophisticated approach to their safeguarding responsibilities. They need to reflect on the changing nature of communication and how this impacts on practice issues, particularly those focused on the identification and assessment of potential risk. To do this successfully, professionals need to recognize that children and young people do not use technology and social media in isolation.
    c. This policy provides some guidance for working practices with children, minimum standards and acceptable use of computing resources and information about our approach to actively teaching safety.
    d. This policy has been developed using resources developed by the City and Hackney Children's Safeguarding Board including, Safeguarding in the Context of Access to Technology and Use of Social Media; and the Minimum standards for professionals.
2. **Our curriculum for teaching about digital safety**
    a. We use the national curriculum programme of study for computing to guide our curriculum. We use the Cambridgeshire Scheme of Work for developing capabilities in relation to e-safety.
    b. By the end of Key Stage one:
        i. Pupils, review their online activity, including maintaining amending online profiles, communication channels and publishing spaces to ensure they do not inadvertently reveal personal details.
        ii. Pupils show respect for content created by others by acknowledging sources, commenting respectfully and responsibly on other people's work and respecting privacy. They are discriminating about what they share and whether any permission is needed to do so.
        iii. Pupils can identify a range of potential online risks including inappropriate contact or content and can identify ways of seeking support and reporting concerns. They exercise caution when receiving attachments and following web links contained in messages.
    c. By the end of Key Stage Two:
        i. Pupils continue to maintain, review and amend online identities, considering the potential impact of these on their digital footprint. They communicate in a wide variety of ways and pay careful attention to what details might be inadvertently revealed
        ii. They engage in an increasing range of online communities safely, respectfully and responsibly both with friends and the wider online community. With adult support, they actively consider and use safety and security settings on a range of digital devices.
        iii. When using online resources and search technologies, pupils are increasingly discerning about what information they gather,

checking the validity of data and showing due respect to privacy and copyright.

iv. Pupils can recognise a range of potential online risks, including inappropriate contact or content and can identify ways of seeking support and reporting concerns.

3. We display the following Digital Safety Class Agreement in each class which is also presented in children's planners and shared at the beginning of each year.

Digital Safety Class Agreement

We agree to:

- use technology to help us learn
- keep passwords and account details private
- log on with our username and password
- use and search for material which is suitable for school
- follow school rules when using computing resources and the internet
- report anything which concern us
- use technology to help create our own work, not copy things

We know that we:

- never reply to messages from unknown senders
- never give out personal information over the internet
- don't use location based services
- never use the internet to find offensive material
- tell an adult if something is wrong
- must think carefully before we share things asking- will this hurt someone's feelings?
- are careful about the information we read on the internet because it might not be accurate- Is the information I'm sharing reliable?
- ask an adult if we are unsure about opening a file

Our teachers must:

- check search terms and use safe search
- show us how to stay safe on the internet using the internet safety resources
- conduct surveys and checks to help us to keep safe online
- be up to date with their knowledge about internet safety

4. **Supervision when children are using digital resources**
   a. Children will always be supervised by members of staff when using devices which can access the internet in school

b. Safe search and appropriate restrictions and filtering are enforced on all school systems.
c. Restrictions for inappropriate content are enabled on all school devises.
d. Children must use their own user name and password to log onto digital resources.
e. Outside of school we recommend children only use devices which can access the internet in a family room.
f. Children should not have touch ID enabled on their phones- parents and carers are advised to supervise and check children's use of online resources.

5. **Reporting abuse and supporting parents**
    a. We actively report abuse to providers and to CEOP. We engage in ongoing dialogue with parents providing annual meetings, information, advice and online guidance.
    b. Our IT service provider is available to enable restrictions or give advice on making children's devices used at home safer. This is a free service.
6. **Social media and platforms provided by school**
    a. The school provides various platforms for children to use, free of charge. All school platforms are restricted to a closed community. For example, children are only able to communicate with other children within our school. They cannot send or receive communications from outside the school community.
    b. We promote the use of school platforms for children to communicate with each other out of school and complete homework.
    c. The school actively advises that children must not have social media accounts before the age of 13. If found, the school reports accounts to the relevant authorities.
    d. Knowledge is power: we advise staff to learn about social media, the latest apps, trends, and potential risks and keep up to date. Technology and social media develop fast - '*Standing still is falling behind'*
7. **Engaging children with discussions about technology**
    a. An informal conversation will often provide a child or young person with the confidence and desire to demonstrate their knowledge of this contemporary area of communication. Initial conversations should be brief and seek to get the child to participate in a discussion about social media in general, not details about their own particular use. The process should include:
        i. **Engage:** Use the Digital Footprint Survey
        ii. **Identify Risks**: Use the Risky Steps Checklist.
        iii. **Assess Understanding**: Use the appropriate guidance for LAC, CSE, Radicalisation, Placement guidance
        iv. **Mitigate Risks**: Use The Safety Steps Checklists.
        v. **Formulate a Plan:** It is important to remember that it is virtually impossible to restrict a child from engaging online. They will be able to access the Internet via a range of devices, apart from phones and traditional desktop PCs and laptops. Even when

access to devices is restricted they often use a friend's device when outside the control or influence of appropriate adults.

8. **Digital footprint survey**
    a. We use an annual digital footprint survey with parents and children to help provide evidence of possible risky use of digital resources and to enable appropriate responses including changes to our curriculum to be made.
    b. The digital footprint survey covers:
        i. Devices used (anything that can access the internet from TVs to gaming consoles, ipods, desktops, laptops, smart phones and tablets
        ii. Platforms used/visited
        iii. Times and location that technology / social media is used
        iv. Levels of Supervision or mitigation strategies applied
    c. Outcomes of the survey are shared with the governing body Curriculum and Pupil Affairs Committee.
    d. Safety checklists from the City and Hackney Children's Safeguarding Board should be used in conjunction with the subject specific 'Prompts' to help focus the identification of risks arising from CSE and radicalisation. This process covers specific questions for children and young people looked after and their carers /placement.
9. **Acceptable use of digital resources in school**
    a. All communication in school is monitored regularly and must be compliant, safe and appropriate for the school setting.
    b. The computer systems within school are made available to children, staff, and other adults to further their education and to enhance professional activities including teaching, research, administration and management. The school's acceptable use policies have been drawn up to protect all parties - the students, the staff, other adults and the school and are reviewed on a regular basis. Staff and other adults wishing to use the schools computer systems, email or Internet will sign a statement to demonstrate they have read and understood this policy.
        i. all Internet activity should be appropriate to the child's education;
        ii. access should only be made via the authorised account and password, which should not be made available to any other person;
        iii. activity that threatens the integrity of the school IT systems or activity that attacks or corrupts other systems is forbidden;
        iv. users are responsible for all e-mail sent and for contacts made that may result in e-mail being received;
        v. all installed software must be authorised by the school business manager;
        vi. use for personal financial gain, gambling, political purposes or advertising is forbidden;
        vii. copyright of materials must be respected;
        viii. posting anonymous messages and forwarding chain letters is forbidden;

ix. as e-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media;
x. use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden.
xi. if you access any site on the internet which you feel is inappropriate, report it to the safeguarding lead immediately.
xii. Be respectful when online and not write or post derogatory or inflammatory information about the school on any social media or attack any pupil, member of staff or member of the school community. This statement is also part of the home-school agreement.
xiii. Further information about the acceptable use of digital resources and technology in realtion to data protection can be found in our Data Protection Policy

10. **Appropriate use of technology and social media by professional working with or for the school**
    a. Only members of staff authorised by the Head teacher may post of social media accounts of the school.
    b. Posting of information, photos or views must be in line with the school's values and shall not make overt reference to any political opinion.
    c. Photos posted may include authorised children but should not associate a child's name with a photograph.
    d. The principles of our code of conduct and safeguarding policies should be applied to all kinds of online communication, including, for example, personal websites and blogs, discussion boards, email groups and instant messaging. It applies to access to social media using any type of internet-enabled device, whether personal or for work.
    e. All school staff are advised that they should not accept or request friendship, follow or accept followers on social media sites of parents at the school. This is an important part of our safeguarding procedures.
    f. When accessing and using social media, employees must ensure that they conduct themselves in a way that reflects positively on the School.
    g. When using social media outside of the work environment, employees should be aware that when posting information, they are not authorized to represent the School or express a view on behalf of the School.
    h. Staff should never reveal information about children, staff or parents in any online social context.
    i. Misuse of schools computer equipment, email or the Internet are serious offences. The school and partners have the right to monitor, inspect and manage the use of the e-mail, Internet services and network resources. This information may be recorded and may be used in disciplinary procedures if necessary.
    j. The ISP and the school reserve the right to disclose any information they deem necessary to satisfy any applicable law, regulation, legal process or governmental request.
    k. The School monitor's compliance with our policy through active searching of files, communication and email including via Google Vault.
    l. Breaches of this policy may result in disciplinary action being taken.