****

**Online Safety Policy**

**Policy Review and Development**

The Online Safety Policy is part of the School Development Plan and relates to other policies, including those for computing, bullying and for child protection. The school’s IT Co-ordinator will also act as the E-Safety Co-ordinator.

This policy has been developed by the IT Coordinator, Kieran Reynolds, and ratified on 07/09/20 by:

* The Headteacher
* Senior leaders
* Class teachers
* Accountability Board

The Online Safety Policy and its implementation will be reviewed annually. This policy will be next reviewed on: 07/09/21

**Scope of the Policy**

This policy applies to all members of the school community, including: staff; students; volunteers; parents and carers; visitors; and community users who have access to and are users of the school ICT systems both in and out of the school.

**Key Responsibilities**

**IT Coordinator:**

The IT Coordinator is responsible for:

* Taking day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policy document, and sharing this policy with other members of staff.
* Ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
* Providing advice for staff.
* Attending online safety training.
* Liaising with school technical staff (Mint IT Support Ltd.).
* Ensure that online safety workshops are held for parents to support them in safeguarding their child.
* Prepare staff with the necessary resources and materials to aid teach and promote online safety.
* Lead assemblies on online safety and discuss current issues.

**Network manager – Mint IT Support Ltd.:**

The network manager is responsible for ensuring that:

* The school’s technical infrastructure is secure and is not open to misuse or malicious attack.
* The school meets required online safety technical requirements.
* Users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
* The filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
* They keep up-to-date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.

**Designated Safeguarding Lead(s) (DSLs):**

DSLs should be trained in Online Safety issues and be aware of the potential for serious child protection or safeguarding issues to arise from:

* Sharing of personal data.
* Access to illegal or inappropriate materials.
* Inappropriate on-line contact with adults or strangers.
* Potential or actual incidents of grooming.
* Cyber-bullying.

**Introduction**

At South Kirkby Academy, we ensure that the safety of all pupils is paramount. This online safety policy recognises the commitment of our school to online safety and acknowledges its part in the school’s overall safeguarding policies and procedures. We recognise that ICT (Information & Communication Technology), the internet and communication online can support children’s development and enrich learning experiences in a technologically evolving world. The increased use of technological devices such as laptops and PCs, mobile phones, tablets, e-readers and gaming devices is becoming commonplace and so it must be a shared responsibility to ensure that children are safeguarded online and know how to use it appropriately. It is therefore essential that professionals (in accordance with ‘Keeping Children Safe in Education’ (DfE, 2015)), parents and children work together to do this. Staff members of South Kirkby Academy have a ‘duty of care’ to ensure that incidents regarding the safety of a young person online are reported as well as educating pupils on how to reduce risk of harm and what to do when they have concerns. As part of our commitment to online safety, we also recognise our obligation to implement a range of security measures to protect the school network and facilities from attack, compromise and inappropriate use and to protect school data and other information assets from loss or damage.

**Aims**

The aims of this online safety policy are as follows:

* Outline the procedures for student’s use of ICT in and out of school
* Raise awareness of good online safety practice
* Set out the key principles expected of all school members of the school community to safeguard children from possible risks and dangers online
* 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
* Define clear structures and processes to deal with inappropriate/illegal activity whilst using digital technology for both teachers and pupils.
* Ensure that pupils are educated about emerging technologies and the dangers posed by the internet in line with school Safeguarding policies.

**Teaching and Learning**

**Why internet use is important?**

The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide children with quality internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

**Internet use will enhance learning**

The school internet access is designed expressly for pupil use and includes filtering appropriate to the age of the pupils. Pupils will be taught what is and is not acceptable internet use. Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

**Pupils will be taught how to evaluate internet content**

The school will ensure that the use of internet derived materials by staff and pupils complies with Copyright Law. Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

**Pupils will be taught the safe use of digital and video images**

Pupils will be made aware of the associated risks with publishing images online. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

**Data Protection**

The school has taken the necessary steps and precautionary measures to ensure compliance with the Data Protection Act 2018 and the current General Data Protection Regulation (GDPR). Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018. The school has a Data Protection policy in place, has an appointed Data Protection Officer and has paid the appropriate fee to the Information Commissioner’s Office (ICO). 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 for which it was collected. Any personal data collected will be for legitimate business interests. All personal data held will be as accurate as possible and inaccuracies will be amended and corrected without unnecessary delay. The school is clear on the arrangements to access personal data and its storage, security and transfer. South Kirkby Academy follows the Waterton Academy Trust’s Freedom of Information (FOI) Policy which conforms to the Freedom of Information Act 2000 and sets out how the school deals with FOI requests. All staff have and will continue to receive training regarding data protection and are aware of their responsibilities.

Staff will ensure that the utmost care is taken to keep personal data safe in order to minimise the risk of its loss or misuse. Therefore, all personal data is encrypted and can only be accessed by authorised members of staff. Staff are aware that they can only see or handle personal data on secure, password-protected computers or devices that offer approved virus and malware checking software and that have been authorised by the Headteacher. These devices must be properly logged-off once they have used or viewed personal data. Personal data that is needed to be transferred electronically must and will be done using encryption. Once the personal data has been transferred or its use is complete, it must be securely deleted from the device.

Breaches of data protection must and will be reported immediately to the ICO by staff and this must be done within 72 hours since its occurrence. Further responses to this will be compliant with GDPR regulations. Parental consent will be sort if the school intends to share personal data, in the interests of legitimate business, with other third parties and those outside of the European Union.

For more information, please refer to the school’s Data Protection Policy.

**Use of Technology – Policy and Procedure**

Pupils will be provided with an Acceptable Use Agreement (see Appendix, Item I) which will outline the school’s rules regarding pupils online activity in school. The Acceptable Use Agreement will be clearly explained to pupils by the staff before they are signed. Once signed, they will be returned and held in school by the IT Coordinator in the event that a breach of these rules is made.

Staff are provided with an Acceptable Use policy that is read, signed and returned to administration. Please refer to the WMAT Online and Social Media Acceptable Use policy for further information. Staff are expected to follow these policies at all times.

Staff must return technology borrowed from the school if they leave the school and user data must be cleared to ensure compliance with GDPR regulations.

**Technical Provision**

The school servers, wireless system and technological devices are managed by Mint IT Support to ensure that the school meets recommended technical safety and security requirements. The servers, wireless systems and cabling are located securely and physical access is restricted. Network health is ensured and protected through use of Windows Defender anti-virus software. In order to guarantee efficiency, technological and network updates are done regularly by Mint IT Support and there will be regular reviews and audits of the safety and security of school technical systems.

All users are provided with their own account (excluding visitors) which requires a username and password to access them. These accounts are also managed by Mint IT Support. Internet is filtered for all pupils by recognised filtering software. This is applied to ensure pupil safety and filters all illegal content as well as terrorist and extremist material. A different level of filtering is applied to staff to allow for reasonable use (illegal content is still filtered). Staff accounts require password changes on a regular basis to increase security. The managed service provider has the ability to monitor users’ searches in support of safeguarding concerns.

**Managing Internet Access**

**E-mail**

* Pupils may only use approved e-mail accounts on the school system and e-mail usage must be supervised and monitored by a staff member.
* Pupils must immediately tell a teacher if they receive an offensive or disturbing e-mail.
* Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission from teaching staff.
* E-mails sent to external organisations should be written carefully and authorised by a member of teaching staff before sending, in the same way as a letter written on school-headed letter.
* The forwarding of chain letters is not permitted.

**Publishing pupils’ images and work on VLE, school website and Twitter**

* Written permission from parents or carers will be obtained before photographs of pupils are published. Permission for this is asked on the child’s enrolment at school.
* Pupils’ work can only be published with the permission of parents.

**Social networking and personal publishing**

* The school will use MINT Support Ltd. to block/filter access to social networking sites. Only teaching staff have access to the school’s Twitter account and the viewing of this social media account is offered only to parents.

**Managing filtering**

* Web content and use is closely monitored and filtered by MINT Support Ltd. To improve their service, the school will work closely alongside MINT Support Ltd. to ensure systems protect pupils by being reviewed.
* If staff or pupils come across unsuitable material online, the site must be reported to the IT Coordinator immediately. Senior staff and the IT Coordinator will ensure that regular filtering tests are made by MINT Support Ltd. to check that the filtering methods selected are appropriate, effective and reasonable.
* Pupils will be informed that all network and internet use will be monitored.
* The use of proxy sites or other means to subvert the school’s filtering system is forbidden, along with the deliberate attempt to access offensive or pornographic material.

**Managing mobile and emerging technologies**

* Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
* \*The senior management team should note that technologies such as mobile phones with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communications. Furthermore, 3G and 4G mobile phones enable users to browse the internet using a different network, meaning that the school would be unable to monitor and filter pupils’ online activity whilst pupils were using these.
* \*For reasons stated above, **pupils’ mobile phones are not permitted on school property** (unless, in exceptional circumstances, permission has been given by the Headteacher, Miss Travis or another member of the Senior Management Team).
* Pupils are given opportunities to experience a range of up-to-date technological devices and will be taught about the safe and appropriate use of these the school’s Online Safety curriculum.

**Directing pupils in lessons where internet use is pre-planned**

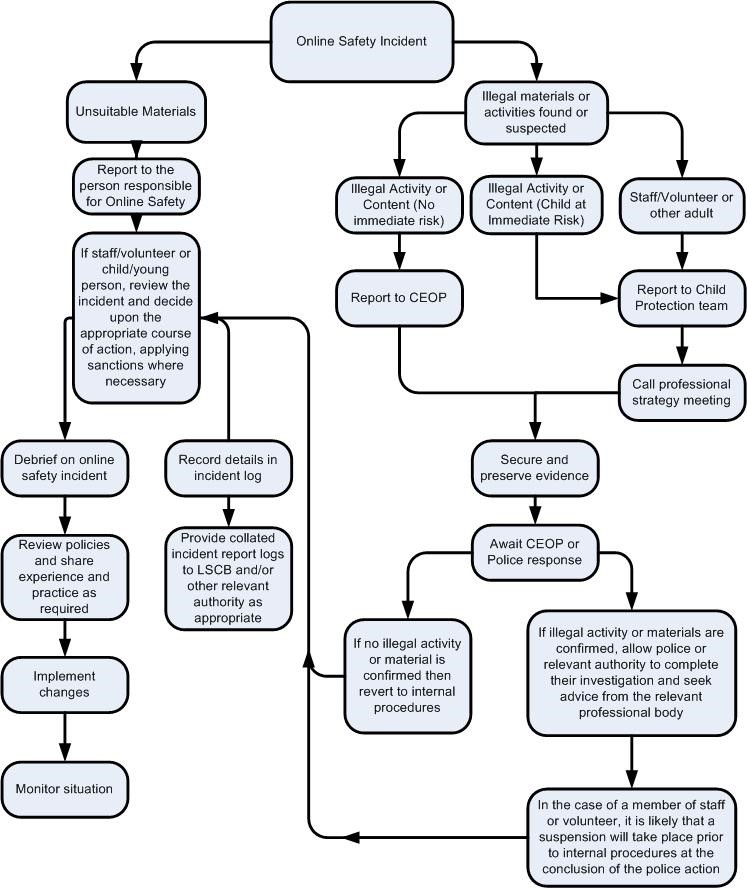
* Pupils will be guided to specific sites that have been checked and approved by an adult.
* Processes will be in place for dealing with unsuitable material that is found during internet searches.

**Communication**

* The sending of offensive, discriminatory, threatening or bullying, and corrupt messages or material, including Youth Produced Sexual Imagery (YPSI) (images, videos, voice recordings, broadcasting, etc.), through any means of technology is forbidden. Users must (in accordance with the school’s Bullying Policy) keep receipt of this communication and report this to a member of staff without responding to this communication.
* The Designated Safeguarding Lead(s) (DSL) will investigate abusive or inappropriate messages or material, including YPSI, and may or may not choose to report it to the police when responding to the incident (this is at the discretion of the Headteacher).
* Pupils are not allowed to access chatrooms or social networking sites in school as these can be sources of inappropriate and harmful behaviour. The risks of using these sites will be addressed through the teaching of the Online Safety curriculum and through PSHE. Despite this, some pupils may be ‘chatting’ outside of school and parents are encouraged to consider taking measures to keep their children safe if using social media.
* Staff are made aware of the expectations of appropriate use of social media and adhere to the Academy Trust Model Social Media Policy for Staff.

**Illegal Incidents**

If there is evidence to suggest illegal activity online, then the school must follow the right hand side of the flowchart (below) for responding to online safety incidents and report immediately to the police.



**School Website and Twitter Page**

South Kirkby Academy recognise the potential for positive, one-way communication to parents, carers and pupils through the school website and further communication to parents and carers through the school’s Twitter page. These are platforms on which the school can give out important messages, key information and celebrate pupils’ learning. However, measures must be in place to prevent the misuse of these and to minimise the risk of harm to pupils, staff and the school. Reasonable steps include ensuring that:

* Formal written permission from parents or carers is gained before referencing or sharing images of them or their children online
* Personal data, including names of pupils and parents or carers who have not given permission for their information to be shared, are not published
* Security settings of both platforms are set at the highest level and checked regularly.
* Issues are reported to the IT Coordinator (including technical issues or unwanted attention and/or contact on the school’s Twitter account)
* Communication is one-way from the school to parents or carers and pupils and that the school does not engage in discussion on these platforms. Instead, staff and parents or carers are to follow the Communications Policy to discuss matters by establishing contact via the school’s telephone number.
* Communication on these platforms complies with the school’s Communication Policy.

**Professional Development**

As stated under the responsibilities of the IT Coordinator, it is their duty to ensure that staff are made aware of online safety updates through staff meetings and professional discussions. The DSLs and the IT Coordinator will receive DSL updates regarding online safety via training and CPD in order to do this.

Teaching and support staff also complete regular safeguarding training modules online that are certified by recognised bodies. It is expected that some staff will identify safety as a training need within their professional review process.

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.

**Online Safety in the Curriculum**

Whilst regulation and technical solutions are very important, it is necessary to ensure that this is balanced by educating pupils to take a responsible approach for their own safety whilst online, both in and out of school.

Online safety should be a focus in all areas of the curriculum and staff should reinforce this message when teaching the school curriculum. The curriculum for online safety will be provided in the following ways:

* Computing, PSHE and other lessons, and assemblies will address online safety issues and will be regularly revisited.
* Pupils will be taught to be critically aware of the online material and content they access.
* Pupils should be taught to respect copyright when using online material.
* Pupils should be supported to build resilience to radicalisation by providing opportunities to discuss controversial issues in a safe environment.
* Pupils will SEND are considered within the online safety curriculum and content is differentiated appropriately.

Possible teaching and learning activities linked to online safety are listed in Appendix 2.

Appendix 3 outlines more useful online resources to teach online safety.

**Supporting Parents with Online Safety**

It is important that parents have a good understanding of the online safety risks and issues as they play an essential role in the education of the children, as well as monitoring their online activity. The school will seek to provide information to parents and carers on how to manage their child’s online behaviour and the associated risks through:

* Curriculum activities
* Informative letters and newsletters, and the school website
* Parents/carers evenings, sessions and online safety workshops
* Safer Internet Day activities
* Online safety workshops and assemblies
* Directing them to relevant websites (e.g. [www.saferinternet.org.uk](http://www.saferinternet.org.uk), <http://www.childnet.com/parents-and-carers> and <https://www.ceop.police.uk/safety-centre/>)

**Appendices**

**Appendix 1: SKA Pupil Acceptable Use Agreement**

****

**South Kirkby Academy Pupil Acceptable Use Agreement**

**In school:**

* I will only use the technology for school purposes.
* I will only use websites and apps in school that have been approved by members of staff.
* I will not tell other people my passwords.
* I will not delete my own or others files.
* I will not download or upload any files without permission from a member of staff.
* I will make sure that I only use web accounts that the school have given me and I will never use anyone else’s web account.
* I will make sure that computer contact with other children and adults is responsible, polite and sensible.
* I will not deliberately look for, save or send anything that is unpleasant or nasty. If I find anything like this, I will tell my teacher or a member of staff immediately.
* I will not try to hide my online activity from the school or IT support company.
* I will keep my own personal details such as my name, phone number or home address to myself and not give them out. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
* I will be responsible for my behaviour when using IT because I know that these rules are to keep me safe.
* I know and understand that the school and the school’s IT support company (MINT Support Ltd.) can check my use of the internet and that my parent(s) or carer(s) will be contacted if there is a concern about my online safety.

**Pupil’s signature:**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Pupil’s full name:**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Class:**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Date:**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Appendix 2: Internet use – Possible teaching and learning activities**

|  |  |  |
| --- | --- | --- |
| **Activities** | **Key online safety issues** | **Relevant websites** |
| Creating web directories to provide easy access to suitable websites. | Pupils should be supervised.  Pupils should be directed to specific, approved online materials. | Web directories commonly used in school – e.g.:  Reading Plus UK; Mathletics; Times Table Rockstars. |
| Using search engines to access information from a range of websites. | Filtering must be active and checked frequently.  Parental consent should be sought.  Pupils should be reminded of safe and responsible use of the internet and what to do if they come across anything that makes them uncomfortable. | Selected, recognised search engines:  CBBC searc; Ask Jeeves for kids; Yahooligans; Kidsclick |
| Publishing pupils’ work on school and other websites. | Pupil and parental consent should be sought prior to publication.  Pupils’ full names and other personal information should be omitted.  Pupils’ work should only be published on moderated sites and by the school administrator. | Making the News  SuperClubs Plus  Headline History  Cluster Microsites  National Education Network  Gallery  SKA website |
| Publishing images | Photographs should not be taken of pupils and they should be approved by a member of staff.  Pupils’ personal information should not be referred to in file names.  Staff must ensure that published images do not breach copyright laws. | Making the news  SuperClubs Plus  Learninggrids  Digital Storytelling  BBC – Primary Art  National Education Network  SKA website |
| Communicating ideas within chat rooms or online forums. | Only chat rooms dedicated to educational use and that are moderated should be used.  Access to other social networking sites should be blocked.  Pupils should never give out personal information – reminders to be given. | SuperClubs Plus  FlashMeeting |

**Appendix 3: Useful resources for teachers**

BBC Stay Safe:

[www.bbc.co.uk/cbbc/help/safesurfing/](http://www.bbc.co.uk/cbbc/help/safesurfing/)

Becta:

<http://schools.becta.org.uk/index.php?section=is>

Chat Danger:

[www.chatdanger.com/](http://www.chatdanger.com/)

Child Exploitation and Online Protection Centre (CEOP):

[www.ceop.gov.uk/](http://www.ceop.gov.uk/)

Childnet:

[www.childnet-int.org/](http://www.childnet-int.org/)

Cyber Café:

<http://thinkuknow.co.uk.co.uk/8_10/cybercafe/cafe/base.aspx>

Digizen:

[www.digizen.org/](http://www.digizen.org/)

Think U Know:

<http://thinkuknow.co.uk.co.uk/>

Safer Children in the Digital World:

[www.dfes.gov.uk/byronreview/](http://www.dfes.gov.uk/byronreview/)