Online Safety Policy 2022-2023

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 safeguarding. The school's IT Co-ordinator will also act as the E-Safety Co-ordinator. This policy was reviewed by the senior leadership team in September 2022.

The Online Safety Policy and its implementation will be reviewed annually. This policy will be next reviewed on: 07/09/23

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

This school is a community and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning, and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

Head of School

It is the responsibility of the Head of School to:

- Support safeguarding leads and technical staff as they review protections for pupils in the home and remote learning procedures, rules and safeguards.
- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding.
- Oversee the activities of the DSL and ensure that their responsibilities listed are being followed and fully supported.
- Ensure that policies and procedures are followed by all staff.
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Local Safeguarding Partnerships.
- Liaise with the DSL on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information.
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the staff, DSL and governors to ensure a GDPR compliant framework for storing data, but helping to ensure that child protection is always put first and data protection processes support careful and legal sharing of information.
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles.

- Ensure that there is a system in place to monitor and support staff (e.g. network manager) who carry out internal technical online-safety procedures.
- Ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety.
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised.
- Ensure the school website meets statutory DfE requirements.

Designated Safeguarding Leads

It is the responsibility of the Designated Safeguarding Lead(s) to:

- "The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety) … this lead responsibility should not be delegated." KCSIE 2022
- Work with the Head of School and technical staff to review protections for pupils in the home and remote learning procedures, rules and safeguards
- Ensure "An effective approach to online safety [that] empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate." KCSIE 2022
- "Liaise with staff (especially pastoral support staff, school nurses, IT Technicians, and SENCOs) on matters of safety and safeguarding (including online and digital safety) and when deciding whether to make a referral by liaising with relevant agencies." KCSIE 2022
- Take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- Remind staff of safeguarding considerations as part of a review of remote learning procedures and technology, including that the same principles of online safety and behaviour apply
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- Work with the head of School, SLT and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Stay up to date with the latest trends in online safety through receiving regular updates in online safety issues and legislation and be aware of local and school trends and undertake Prevent awareness training
- Review and update this policy, other online safety documents and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the governors.
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles
- Ensure that online safety education is embedded across the curriculum and beyond, in wider school life
- Promote an awareness and commitment to online safety throughout the school community, with a strong focus on parents
- Liaise with school technical, pastoral, and support staff as appropriate
- Communicate regularly with SLT and the designated safeguarding governor to discuss current issues (anonymised), review incident logs and appropriate filtering and monitoring
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident
- Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- Maintain up-to-date documentation of the school's online security and technical procedures
- Ensure adequate provision for staff to flag issues when not in school and for pupils to disclose issues when off site, especially when in isolation/quarantine/lockdown
- Oversee and discuss 'appropriate filtering and monitoring' with governors (is it physical or technical?) and ensure staff are aware

- Ensure the 2018 DfE guidance on sexual violence and harassment is followed throughout the school and that staff adopt a zero-tolerance approach to this, as well as to bullying

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.

Governing Body, led by the Safeguarding Governor

It is the responsibility of the Governing Body, led by the Safeguarding Governor to:

- Approve this policy and strategy and subsequently review its effectiveness, e.g. by asking the questions in the helpful document from the UK Council for Child Internet Safety (UKCIS) Online safety in schools and colleges: Questions from the Governing Board.
- Ask about how the school has reviewed protections for pupils in the home (including when with online tutors) and remote-learning procedures, rules and safeguards
- "Ensure an appropriate senior member of staff, from the school leadership team, is appointed to the role of DSL [with] lead responsibility for safeguarding and child protection (including online safety) [with] the appropriate status and authority [and] time, funding, training, resources and support…" KCSIE 2022
- Support the school in encouraging parents and the wider community to become engaged in online safety activities
- Have regular strategic reviews with the DSL and incorporate online safety into standing discussions of safeguarding at governor meetings
- Work with the DSL and head of school to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Check all school staff have read Part 1 and Annex A of KCSIE; check Annex C on Online Safety reflects practice in your school
- Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction.
- The training should be regularly updated […] in line with advice from the local three safeguarding partners […] integrated, aligned and considered as part of the overarching safeguarding approach.
- "Ensure appropriate filters and appropriate monitoring systems are in place [but…] be careful that 'overblocking' does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding". KCSIE 2022
- "Ensure that children are taught about safeguarding, including online safety […] as part of providing a broad and balanced curriculum […] Consider a whole school approach to online safety [with] a clear policy on the use of mobile technology." In-line with 'Teaching Online Safety in Schools 2019' and the UKCIS cross-curricular framework 'Education for a Connected World' to support a whole-school approach.

All Staff

It is the responsibility of all staff to:

- Pay particular attention to safeguarding provisions for home-learning and remote-teaching technologies.
- Recognise that RSE has been extended and that it is a whole-school subject requiring the support of all staff; online safety has become core to this new subject
- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job
- Know who the Designated Safeguarding Lead (DSL) is and the Deputy DSLs are
- Read Part 1 and Annex A and have been sign posted to Annex C of KCSIE 2021
- Read and follow this policy in conjunction with the school's main safeguarding policy
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures.
- Sign and follow the staff acceptable IT use policy
- Notify the DSL if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon
- Identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the RSE curriculum, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)
- Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites
- When supporting pupils remotely, be mindful of additional safeguarding considerations
- To carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law
- Prepare and check all online source and resources before using within the classroom
- Encourage pupils to follow their acceptable use policy, at home as well as at school and remind them about it and enforce school procedures if not followed
- Notify the DSL of new trends and issues before they become a problem
- Take a zero-tolerance approach to bullying and low-level sexual harassment
- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and violence) in the playground, corridors, toilets and other communal areas outside the classroom – always report to the DSL
- Receive regular updates from the DSL and have a healthy curiosity for online safety issues
- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff.

IT (& Computing) Lead:

It is the responsibility of the IT (& Computing) Lead to:

- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Support the HT and DSL team as they review protections for pupils in the and remote-learning procedures, rules and safeguards
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements
- Work closely with the DSL to ensure that school systems and networks reflect school policy
- Ensure all stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc)
- Support and advise on the implementation of 'appropriate filtering and monitoring' as decided by the DSL and SLT with support from Mint Support Ltd.
- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls
- With the support of the DSL, monitor the use of school technology, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with school policy
- Maintain up-to-date documentation of the school's online security and technical procedures
- Work closely with the DSL to ensure they understand who the nominated contacts are, what they can do and what data access they have, as well as the implications of all existing services and changes to settings that you might request (for example: for YouTube restricted mode, internet filtering settings, firewall port changes, pupil email settings, and sharing settings for any cloud services such as Microsoft Office 365 and Microsoft Teams).
- Attend up-to-date online safety training.
- Lead assemblies on online safety and discuss current issues.

PSHE Lead:

It is the responsibility of the PSHE Lead to:

- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE / Relationships education and health education curriculum. "This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their pupils' lives." KCSIE 2022
- This will complement the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE.

External groups:

- Any external individual/organisation will sign an acceptable use policy prior to using technology or the internet within school and out of school when promoting the school
- Support the school in promoting online safety and data protection
- Model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers

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.

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, 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 Head of School. 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.

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 WAT 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.

Social media incidents

Breaches of this policy and of school AUPs (Acceptable Use Policies) will be dealt with in line with the school behaviour policy (for pupils) or code of conduct/handbook (for staff). Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, we will request that the post be deleted and will expect this to be actioned promptly. Where an offending post has been made by a third party, the school may report it to the platform where it is hosted, and may contact the Professionals' Online Safety Helpline (run by the UK Safer Internet Centre) for support or help to accelerate this process. The police or other authorities may be involved where a post is potentially illegal or dangerous.

Extremism

The school has obligations relating to radicalisation and all forms of extremism under the Prevent Duty (see Safeguarding Policy). Staff will not support or promote extremist organisations, messages or individuals, give them a voice or opportunity to visit the school, nor browse, download or send material that is considered offensive or of an extremist nature by the school. We ask for parents' support in this also, especially relating to social media, where extremism and hate speech can be widespread on certain platforms.

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

- KCSIE 2022 obliges schools to "ensure appropriate filters and appropriate monitoring systems are in place and not be able to access harmful or inappropriate material but at the same time be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."
- 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 Lead 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 devices with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communications. Furthermore, 3G, 4G and 5G-ready mobile devices 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 Head of School or another member of the Senior Management Team. If parents require children to bring mobile phones for use on the journey to and from school these will be stored in the main school office during the school
- 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 Head of School).
- 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 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.

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, 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.

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.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.	SuperClubs Plus FlashMeeting