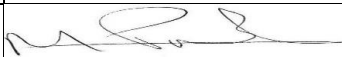


Date approved	January 2022	Approved by	Executive Headteacher
Review cycle	2 year	Signature	
Date for review	January 2024	Author	Jemma Tague

1. Scope

1.1 This policy applies to all stakeholders including students

2. Principles

2.1 Kingsmead and Newton's Walk (The School) values the dignity of every individual member of staff and will apply this policy fairly and consistently in line with its core values of RESPECT and SHINE. We will explore reasonable adjustments in applying this procedure to employees with a disability.

3. Statement of Intent

3.1 The School understands that using online services is an important aspect of raising educational standards, promoting pupil achievement and enhancing teaching and learning.

3.2 The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

3.3 The breadth of issues classified within online safety is considerable, but they can be categorised into three areas of risk:

Content: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, and racist or radical and extremist views.

Contact: Being subjected to harmful online interaction with other users, e.g. commercial advertising and adults posing as children or young adults.

Conduct: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.

3.4. The measures implemented to protect pupils and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

4. Roles and responsibilities

4.1 The **governing board** is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training at induction.
- Ensuring that there are appropriate filtering and monitoring systems in place.

4.2 The **headteacher** is responsible for:

- Supporting the DSL and any deputies by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.

- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
- Working with the DSL and ICT leaders and IT Providers to conduct half-termly light-touch reviews of this policy and practice.
- Working with the DSL and governing board to update this policy on a regular basis.

4.3 The **DSL and ICT Leader** is responsible for:

- Taking the lead responsibility for online safety in the school.
- Acting as the named point of contact within the school on all online safeguarding issues.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND and vulnerable learners face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and ICT technicians.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring appropriate referrals are made to external agencies, as required.
- Staying up-to-date with current research, legislation and online trends.
- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff.
- Ensuring all members of the school community understand the reporting procedure for a concern.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- Reporting to the governing board about online safety.
- Working with the headteacher, ICT Leader and ICT provider to conduct half-termly light-touch reviews of this policy.
- Working with the headteacher and governing board to update this policy on a regular basis.

4.4 **ICT Provider** are responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the headteacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.
- Working with the DSL to conduct half-termly light-touch reviews of this policy.

4.5. All staff members are responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviors.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

4.6 Pupils are responsible for:

- Respect the feelings and rights of others both off and online
- Adhering to this policy, the **Acceptable Use Agreement** and other relevant policies.
- Seeking help from school staff if they are concerned about something they or a peer has experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.
- Responsible for contributing to the development of online safety

4.7 Parents are responsible for:

- Upholding the homes school agreement

5. The curriculum

5.2 Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

- PSHE including RSE & Health education
- ICT

5.3 The curriculum and the school's approach to online safety is developed in line with the UK Council for Child Internet Safety's 'Education for a Connected World' framework and the DfE's 'Teaching online safety in school' guidance.

5.4 Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using.

5.5 Online safety teaching is always appropriate to pupils' ages and developmental stages.

5.6 The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support

5.7 The online risks pupils may face online are always considered when developing the curriculum. The risks that are considered and how they are covered in the curriculum can be found in [Appendix 1](#) of this policy.

5.8 The DSL is involved with the development of the school's online safety curriculum.

5.9 The school recognises that, while any pupil can be vulnerable online, there are some pupils who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. pupils with SEND and LAC. Relevant members

of staff, e.g. the SENCO and designated teacher for LAC, work together to ensure the curriculum is tailored so these pupils receive the information and support they need.

5.10 Class teachers review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils. When reviewing these resources, the following questions are asked:

- Where does this organisation get their information from?
- What is their evidence base?
- Have they been externally quality assured?
- What is their background?
- Are they age appropriate for pupils?
- Are they appropriate for pupils' developmental stage?

5.11 External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The **headteacher, ICT Leader and DSL** decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate. (see external visitors policy for further guidance)

5.12 Before conducting a lesson or activity on online safety, the class teacher and DSL consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The DSL advises the staff member on how to best support any pupil who may be especially impacted by a lesson or activity.

5.13 Lessons and activities are planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

5.14 During an online safety lesson or activity, the class teacher ensures a safe environment is maintained in which pupils feel comfortable to say what they feel and are not worried about getting into trouble or being judged.

5.15 If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will report this through the agreed channels of the school

5.16 If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure agreed in school

6. Staff training

6.2 All staff receive safeguarding and child protection training, which includes online safety training, during their induction.

6.3 Online safety training for staff is updated **regularly** and is delivered in line with advice from local and national safeguarding partners.

6.4 In addition to this training, staff also receive regular online safety updates as required and at least annually from the **DSL** and/or **ICT Leader**.

6.5 The DSL and any deputies undergo training to provide them with the knowledge and skills they need to carry out their role, this includes online safety training. This training is updated at least every two years.

6.6 In addition to this formal training, the DSL and any deputies receive regular online safety updates to allow them to keep up with any developments relevant to their role. In relation to online safety, these updates allow the DSL and their deputies to:

- Understand the unique risks associated with online safety and be confident that they have the relevant knowledge and capability required to keep pupils safe while they are online at school.
- Recognise the additional risks that pupils with SEND face online and offer them support to stay safe online.

6.7 Staff are required to adhere to the **Staff Code of Conduct** at all times, which includes provisions for the acceptable use of technologies and the use of social media.

6.8 All staff are informed about how to report online safety concerns

6.9 The staff within school, Pastoral leads, act as the first point of contact for staff requiring advice about online safety.

7. Educating parents

7.2 The school works in partnership with parents to ensure pupils stay safe online at school and at home.

Parents are provided with information about the school's approach to online safety and their role in protecting their children. Parental awareness is raised in the following ways:

Parents' evenings

- Twilight training sessions
- Newsletters

7.3 Parents are given a copy of the Acceptable Use Agreement at induction and is discussed with the child and parent to ensure their child understands the document and the implications of not following it.

8. Classroom use

8.2 A wide range of technology is used during lessons, including the following:

- Computers
- Laptops
- Tablets
- Internet
- Email
- Cameras

8.3 Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher always reviews and evaluates the resource.

8.4 Class teachers ensure that any internet-derived materials are used in line with copyright law.

8.5 Pupils are supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

9. Internet access

9.2 Pupils, staff and other members of the school community are only granted access to the school's internet network once they have read and signed the Acceptable Use Agreement.

9.3 A record is kept of users who have been granted internet access in pupil electronic file (induction).

9.4 All members of the school community are encouraged to use the school's internet network, instead of 3G, 4G and 5G networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

10. Filtering and monitoring online activity

10.2 The ICT Provider ensures the school's ICT network has appropriate filters and monitoring systems in place.

10.3 The SBM undertake a risk assessment to determine what filtering and monitoring systems are required.

- 10.4 The filtering and monitoring systems the school implements are appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks.
- 10.5 The governing board ensures 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.
- 10.6 The SBM undertake monthly checks on the filtering and monitoring systems to ensure they are effective and appropriate.
- 10.7 Requests regarding making changes to the filtering system are directed to the headteacher.
- 10.8 Prior to making any changes to the filtering system, Headteacher and the SBM conduct a risk assessment.
- 10.9 Any changes made to the system are recorded by ICT Provider
- 10.10 Reports of inappropriate websites or materials are made to DSL immediately, who investigates the matter and makes any necessary changes.
- 10.11 Deliberate breaches of the filtering system are reported to the DSL and ICT Leader, who will escalate the matter appropriately.
- 10.12 If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Policy.
- 10.13 If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure and/or LADO.
- 10.14 If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.
- 10.15 The school's network and school-owned devices are appropriately monitored.
- 10.16 All users of the network and school-owned devices are informed about how and why they are monitored.

11. Network security

- 11.2 Technical security features, such as anti-virus software, are kept up-to-date and managed by ICT Provider.
- 11.3 Firewalls are switched on at all times.
- 11.4 ICT Provider review the firewalls on a regular basis to ensure they are running correctly, and to carry out any required updates.
- 11.5 Staff and pupils are advised not to download unapproved software or open unfamiliar email attachments.
- 11.6 Staff members and pupils report all malware and virus attacks to the ICT Provider.
- 11.7 All members of staff have their own unique usernames and private passwords to access the school's systems.
- 11.8 Pupils are provided with their own unique username and private passwords.
- 11.9 Staff members and pupils are responsible for keeping their passwords private.
- 11.10 Passwords have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible.
- 11.11 Users are not permitted to share their login details with others and are not allowed to log in as another user at any time.
- 11.12 Users are required to lock access to devices and systems when they are not in use.
- 11.13 Users inform ICT Provider if they forget their login details, who will arrange for the user to access the systems under different login details.

- 11.14 If a user is found to be sharing their login details or otherwise mistreating the password system, the headteacher is informed and decides the necessary action to take.

12. Emails

- 12.2 Access to and the use of emails is managed in line with the Data Protection Policy, Acceptable Use Agreement, the Schools Code of Conduct and Confidentiality Policy.
- 12.3 Staff and pupils are given approved school email accounts and are only able to use these accounts at school and when doing school-related work outside of school hours.
- 12.4 Prior to being authorised to use the email system, staff and pupils must agree to and sign the relevant acceptable use agreement.
- 12.5 Personal email accounts are not permitted to be used on the school site.
- 12.6 Any email that contains sensitive or personal information is only sent using secure and encrypted email.
- 12.7 Staff members and pupils are required to block spam and junk mail, and report the matter to ICT provider.
- 12.8 The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff and pupils are made aware of this.
- 12.9 Chain letters, spam and all other emails from unknown sources are deleted without being opened.
- 12.10 The ICT curriculum team should explain what a phishing email and other malicious emails might look like – this assembly includes information on the following:
- How to determine whether an email address is legitimate
 - The types of address a phishing email could use
 - The importance of asking “does the email urge you to act immediately?”
 - The importance of checking the spelling and grammar of an email

13. Social networking

13.1 Personal use

- 13.2 Access to social networking sites is filtered as appropriate.
- 13.3 Staff and pupils are not permitted to use social media for personal use during lesson time.
- 13.4 Staff members are advised that their conduct on social media can have an impact on their role and reputation within the school.
- 13.5 Staff receive regular training on how to use social media safely and responsibly.
- 13.6 Staff are not permitted to communicate with pupils or parents over social networking sites and are reminded to alter their privacy settings to ensure pupils and parents are not able to contact them on social media.
- 13.7 Pupils are taught how to use social media safely and responsibly through the online safety curriculum.
- 13.8 Concerns regarding the online conduct of any member of the school community on social media are reported to the DSL and managed in accordance with the relevant policy, e.g. Anti-Bullying Policy, Staff Code of Conduct and Behaviour Policy.
- 13.9 The school's official social media channels are only used for official educational or engagement purposes.
- 13.10 Staff members must be authorised by the headteacher to access to the school's social media accounts.
- 13.11 All communication on official social media channels by staff on behalf of the school is clear, transparent and open to scrutiny.

13.12 The Staff Code of Conduct contains information on the acceptable use of social media – staff members are required to follow these expectations at all times.

14. The school website

14.2 The Governing Body is responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

14.3 The website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law.

14.4 Personal information relating to staff and pupils is not published on the website.

15. Managing reports of online safety incidents

15.2 Staff members and pupils are informed about what constitutes inappropriate online behaviour in the following ways:

- Staff training
- The online safety curriculum
- Key Working Sessions
- New Staff Induction
- The Safeguarding Newsletter

15.3 Concerns regarding a staff member's online behaviour are reported to the headteacher who decides on the best course of action in line with the relevant policies, e.g. Staff Code of Conduct, Allegations of Abuse Against Staff Policy and Disciplinary Policy and Procedures.

15.4 Concerns regarding a pupil's online behaviour are reported through safeguarding procedures

15.5 Concerns regarding a pupil's online behaviour are dealt with in accordance with relevant policies depending on their nature, e.g. Behaviour Policy and Child Protection and Safeguarding Policy.

15.6 Where there is a concern that illegal activity has taken place, the headteacher contacts the police, and IWF and/or CEOP.

All online safety incidents and the school's response are recorded on CPOMS

16. Responding to specific online safety concerns

Cyberbullying

16.2 Cyberbullying, against both pupils and staff, is not tolerated.

16.3 Any incidents of cyberbullying are dealt with quickly and effectively whenever they occur.

16.4 The school recognises that peer-on-peer abuse can take place online. Examples include the following:

- Non-consensual sharing of sexual images and videos
- Sexualised cyberbullying
- Online coercion and threats
- Unwanted sexual comments and messages on social media
- Online sexual exploitation

16.5 The school responds to all concerns regarding online peer-on-peer abuse, whether or not the incident took place on the school premises or using school-owned equipment.

16.6 Concerns regarding online peer-on-peer abuse are reported to the DSL who will investigate the matter with other senior colleagues

Upskirting

- 16.7 Under the Voyeurism (Offences) Act 2019, it is an offence to operate equipment and to record an image beneath a person's clothing without consent and with the intention of observing, or enabling another person to observe, the victim's genitals or buttocks (whether exposed or covered with underwear), in circumstances where their genitals, buttocks or underwear would not otherwise be visible, for a specified purpose.
- 16.8 A "specified purpose" is namely:
- Obtaining sexual gratification (either for themselves or for the person they are enabling to view the victim's genitals, buttocks or underwear).
 - To humiliate, distress or alarm the victim.
- 16.9 "Operating equipment" includes enabling, or securing, activation by another person without that person's knowledge, e.g. a motion activated camera.
- 16.10 Upskirting is not tolerated by the school.
- 16.11 Incidents of upskirting are reported to the DSL who will then decide on the next steps to take, which may include police involvement, in line with the Safeguarding Policy.

Youth produced sexual imagery (sexting)

- 16.12 Youth produced sexual imagery is the sending or posting of sexually suggestive images of under-18s via mobile phones or over the internet. Creating and sharing sexual photos and videos of individuals under 18 is illegal.
- 16.13 All concerns regarding sexting are reported to the DSL.
- 16.14 Following a report of sexting, the following process is followed:
- The DSL holds an initial review meeting with appropriate school staff
 - Subsequent interviews are held with the pupils involved, if appropriate
 - Parents are informed at an early stage and involved in the process unless there is a good reason to believe that involving the parents would put the pupil at risk of harm
 - At any point in the process if there is a concern a pupil has been harmed or is at risk of harm, a referral will be made to children's social care services and/or the police immediately
 - The interviews with staff, pupils and their parents are used to inform the action to be taken and the support to be implemented
- 16.15 When investigating a report, staff members do not view the youth produced sexual imagery unless there is a good and clear reason to do so.
- 16.16 If a staff member believes there is a good reason to view youth produced sexual imagery as part of an investigation, they discuss this with the headteacher first.
- 16.17 The decision to view imagery is based on the professional judgement of the DSL and/or the headteacher and always complies with the Safeguarding Policy.
- 16.18 Any accidental or intentional viewing of youth produced sexual imagery that is undertaken as part of an investigation is recorded.
- 16.19 If it is necessary to view the imagery, it will not be copied, printed or shared.

Online abuse and exploitation

- 16.20 Through the online safety curriculum, pupils are taught about how to recognise online abuse and where they can go for support if they experience it.
- 16.21 The school responds to concerns regarding online abuse and exploitation, whether or not it took place on the school premises or using school-owned equipment.
- 16.22 All concerns relating to online abuse and exploitation, including child sexual abuse and exploitation and criminal exploitation, are reported to the DSL and dealt with in line with the Safeguarding Policy.

Online hate

16.23 The school does not tolerate online hate content directed towards or posted by members of the school community.

16.24 Incidents of online hate are dealt with in line with the relevant school policy depending on the nature of the incident and those involved, e.g. Staff Code of Conduct, Anti-Bullying Policy and Code of Conduct.

Online radicalisation and extremism

16.25 The school's filtering system protects pupils and staff from viewing extremist content.

16.26 Concerns regarding a staff member or pupil being radicalised online are dealt with in line with the Child Protection and Safeguarding Policy and Prevent Duty Policy.

Appendix A

Esafety Topics covered in ICT

- Understand the risks and solutions of **cyber bullying** and **peer on peer abuse**
- Understand the meaning of E-Safety
- Identify the advantages and disadvantages of E-Safety
- Understand the risks and solutions of **online grooming**
- Explain the impact of Social Media on society
- Identify the advantages and disadvantages of E-Safety
- Learn the dangers and solutions of social media sites and chat rooms
- Explain the impact of having a mobile phone
- Identify the advantages and disadvantages of a mobile phone
- Learn the dangers and solutions of having and using a mobile phone and sexting
- Understand the different effects that can cause harm to your computer or device
- Understand how to keep your computer/device and yourself safe

Understand the meaning, dangers and solutions of:

Spam , Viruses, Fraud and Phishing

- Identify common types of computer crime
- Look at examples of computer crime on the Internet
- Learn about different types of email scam,
- Recognise the signs of fraudulent emails
- Learn about the Computer Misuse Act – which makes certain activities illegal
- Look at examples of computer misuse
- Understand what is meant by hacking
- Understand what is meant by malware
- Learn ways to protect yourself from malware and hacking
- Be aware of who might hold personal data about you
- Discuss the need for various organisations to hold data about you
- Be aware of the possibility of identity theft
- Know how to minimize the chance of identity theft
- Learn about Copyright law, what it says and what it means
- Look at examples of copyright infringement
- Understand the damage that illegal copying does to individuals, companies and society
- Compare copyright infringement with plagiarism
- Managing Online Information- Fake news
- Using effective tools for finding information
- Advantages and disadvantages of ecommerce

Privacy and Security

- Learning about Online scams and how to protect
- Learning about keeping personal data secure
- Brief overview about hacking and how to protect
- Importance of secure passwords
- Social engineering
- Identify security issues that might threaten system performance
- Take appropriate security precautions to protect IT systems and data
- Identify threats to information security associated with widespread use of technology
- Take appropriate precautions to keep information secure
- Follow relevant guidelines and procedures for the secure use of IT
- Explain why it is important to backup data securely
- Ensure that my personal data is backed up to appropriate media

Online Reputation

- Importance of Online reputation
- Ethical and legal issues