Thorpe St Andrew School and Sixth Form

E-Safety Policy

Reviewed - **February 2020**

Next Review - **February 2021**

Policy Consultation and Review

This policy has been updated in line with the requirements of the General Data Protection Regulation (GDPR), which came into effect on 25 May 2018, to include further information on consent, data security and the responsibilities of the Data Protection Officer (DPO). The updated policy also includes reference to the 2019 version of '*Keeping Children Safe in Education*'.

Contents

Page No.

Statement of Intent

At Thorpe St Andrew School and Sixth Form, we understand that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open up opportunities for students and play an important role in their everyday lives.

Whilst the school recognises the importance of promoting the use of computer technology throughout the curriculum, we also understand the need for safe internet access and appropriate use.

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 students and staff.

The school is committed to providing a safe learning and teaching environment for all students and staff, and has implemented important controls to mitigate the risk of harm.

The E-Safety Office is the Designated Safeguarding Lead in the Senior Leadership Team.

1. LEGAL FRAMEWORK

1.1 This policy has due regard to all relevant legislation including, but not limited to:

- The General Data Protection Regulation (GDPR);
- Freedom of Information Act 2000.

1.2 This policy also has regard to the following statutory guidance:

- DfE *'https://www.gov.uk/government/publications/keeping-children-safe-in-education--2 ;*
- National Cyber Security Centre 2017 *'https://www.ncsc.gov.uk/collection/small-business-guide*
- Teaching online safety in school - non-statutory guidance.

1.3 This policy will be used in conjunction with the following school Thorpe St Andrew School and Sixth Form (TSAS) and the Yare Education Trust (YET) policies and procedures:

- Whole School Policy for Safeguarding Children, Incorporating Child Protection - (TSAS);
- Anti-Bullying including Cyber Bullying Policy - (TSAS);
- Social Media Policy - (YET);
- Allegations of Abuse Against Staff Policy - (YET);
- Acceptable Use Agreement - (TSAS);
- IT and Acceptable Use Policy - (YET);
- Data Security Breach Prevention and Management Plan - (YET);
- Behaviour for Learning Policy - TSAS.

2. USE OF THE INTERNET

2.1 The school understands that using the internet is important when raising educational standards, promoting student achievement and enhancing teaching and learning.

2.2 Internet use is embedded in the statutory curriculum and is therefore an entitlement for all students, though there are a number of controls the school is required to implement to minimise harmful risks.

2.3 When accessing the internet, individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful, including the following:

- Access to illegal, harmful or inappropriate images;
- Cyber bullying;
- Access to, or loss of, personal information;
- Access to unsuitable online videos or games;
- Loss of personal images;
- Inappropriate communication with others;
- Illegal downloading of files;
- Exposure to explicit or harmful content, for example , content involving radicalisation;
- Plagiarism and copyright infringement;
- Sharing the personal information of others without the individual's consent or knowledge.

3. ROLES AND RESPONSIBILITIES

3.1 It is the responsibility of all staff to be alert to possible harm to students or staff due to inappropriate internet access or use, both inside and outside of the school, and to deal with incidents of such as a priority.

3.2 The E-Safety Officer is responsible for ensuring that there are appropriate filtering and monitoring systems in place to safeguard students.

3.3 The E-Safety Officer (Assistant Principal/Designated Safeguarding Officer), is responsible for ensuring the day-to-day E-Safety in the school and managing any issues that may arise.

3.4 The Principal is responsible for ensuring that the E-Safety Officer and any other relevant staff receive CPD to allow them to fulfil their role and train other members of staff.

3.5 The E-Safety Officer will provide all relevant training and advice for members of staff as part of the requirement for staff to undergo regularly updated safeguarding training and be able to teach students about online safety.

3.6 The E-Safety Officer will regularly monitor the provision of E-Safety in the school and will provide feedback to the Principal.

3.7 The Principal will establish a procedure for reporting incidents and inappropriate internet use, either by students or staff. This procedure is CPOMS.

3.8 The E-Safety Officer will ensure that all members of staff are aware of the procedure when reporting E-Safety incidents, which will be recorded on CPOMS.

3.9 The IT team and E-Safety Officer will where possible, monitor staff use of social media, and will justify all instances of monitoring to ensure that it is necessary and outweighs the need for privacy.

3.10 The **Governing Board** will meet each term with the E-Safety Officer to discuss the effectiveness of the E-Safety provision, current issues, and to review logs, as part of the school's duty of care. This will be a standing agenda item at each Students and Community committee meeting.

3.11 The **Governing Board** will evaluate and review E-Safety on a **termly** basis, considering the latest developments in ICT and any concerns raised by students and staff.

3.12 The Principal will review and amend this policy with the E-Safety Officer and Data Protection Officer, taking into account new legislation, government guidance and previously reported incidents, to improve procedures on an annual basis.

3.13 Curriculum Leaders, in all departments, are responsible for ensuring that E-Safety issues are promoted in the curriculum. Teachers are responsible for ensuring that internet access is promoted at all times.

3.14 All staff are responsible for ensuring they are up-to-date with current E-Safety issues, and this E-Safety policy.

3.15 All staff and students will ensure they understand and adhere to the school's **Acceptable Use Agreement**, which they virtually sign each time they log on to the school's systems.

3.16 Parents are responsible for ensuring their child understands how to use computer technology and other digital devices appropriately.

3.17 The Principal is responsible for communication with parents regularly and updating them on current E-Safety issues and control measures via Newsletters and briefings.

3.18 All students are aware of their responsibilities regarding the use of school-based ICT systems and equipment, including their expected behaviour, through the acceptable usage agreement each time they log on.

4. E-SAFETY EDUCATION

4.1 An E-Safety programme is established and taught across the curriculum on a regular basis, ensuring that students are aware of the safe use of new technology both inside and outside of the school.

4.2 Students will be taught about the importance of E-Safety and are encouraged to be critically aware of the content they access online, including extremist material, and the validity of website content.

4.3 Students will be taught to acknowledge ownership of information they access online, in order to avoid copyright infringement and/or plagiarism.

4.4 Clear guidance on the use of the internet in school will be presented across the school.

4.5 Students are instructed to report any suspicious use of the internet and digital devices to their classroom teacher or BEST.

4.6 PSHE lessons will be used to educate students about cyber bullying, including how to report cyber bullying, the social effects of spending too much time online and where to access help.

4.7 Lessons will be delivered in an age and contextual appropriate way. Lessons will be differentiated based on learner needs, experiences and exposure they have to an online environment. Many learners with SEND will want to engage in the same activities as their peers but may lack the understanding, skills or support to do this safely.

The SENDCo will understand the needs of learners with SEND and deliver differentiated curriculum within intervention lessons, on an annual basis or more often if deemed appropriate.

4.8 The school will hold E-Safety events, such as assemblies, ethos activities, Safer Internet Day (February 2020) and Anti-Bullying week, to promote online safety.

Educating Staff:

4.9 E-Safety training opportunities are available to all staff members, including whole school activities and CPD training courses, in line with the Safeguarding training. Details of training and information on E-Safety will be publicised on the school Messenger (internal staff newsletter) and discussed in briefings.

4.10 All staff will undergo E-Safety training on an annual basis to ensure they are aware of current E-Safety issues and any changes to the provision of E-Safety, as well as current developments in social media and the internet as a whole.

4.11 All staff will undergo regular audits by the E-Safety Officer in order to identify areas of training need.

4.12 All staff will employ methods of good practice and act as role models for students when using the internet and other digital devices.

4.13 All staff are reminded of the importance of acknowledging information they access online, in order to avoid copyright infringement and/or plagiarism.

4.14 Any new staff are required to undergo E-Safety training as part of their induction programme into Safeguarding and Child Protection, ensuring they fully understand this E-Safety policy.

4.15 The E-Safety Officer will act as the first point of contact for staff requiring E-Safety advice.

Education of Parents:

4.17 E-Safety information will be directly delivered to parents through a variety of formats, including Newsletters, the school website and social media.

4.18 Parent Consultation Evenings, meetings and other similar occasions will be utilised to inform parents of any E-Safety related concerns.

5. E-SAFETY CONTROL MEASURES

Internet access:

5.1 Where a student is over the age of 13 and they fully understand what they are consenting to, parents' consent is not required in line with the GDPR; however, the school will notify parents that students consent independently by logging on and accepting the user agreement.

5.2 All students will be provided with passwords and will be instructed to keep these confidential.

5.3 Students' passwords will expire every **90** days, and their activity is continuously monitored by the ICT team.

5.4 Management systems will be selective, on request via remote viewing software, to allow teachers and members of staff to control workstations and monitor students' activity.

5.5 Effective filtering systems will be established to minimize any potential risks to students through access to, or trying to access, certain websites which are harmful or use inappropriate material.

5.6 Filtering systems will be used which are relevant to students' age ranges, their frequency of use of ICT systems, and the proportionality of costs compared to risks.

5.7 The **Governing Board** will ensure that the use of appropriate filters and monitoring systems does not lead to 'over blocking' - unreasonable restrictions as to what students can be taught with regards to online teaching and safeguarding.

5.8 Any requests by staff for websites to be added or removed from the filtering list must be first enabled by the IT Support team.

5.9 All school systems will be protected by up-to-date virus software.

5.10 An agreed procedure will be in place for the provision of temporary users, for example Supply Staff.

5.11 Staff are able to use the internet for personal use within the professional standards accepted for teaching for non-personal activities.

5.13 Personal use will only be monitored by the ICT team for access to any inappropriate or explicit sites, where the need to do so outweighs the need for privacy.

5.14 Inappropriate internet access by staff may result in the staff member being permitted to use the internet for school purposes only and prohibited from using any personal devices. This will be dealt with following the process outlined in the **misuse by staff** section of this policy.

Email:

5.15 Students and staff will be given approved email accounts.

5.16 The use of personal email accounts to send and receive personal data or information is prohibited.

5.17 No sensitive personal data shall be sent to any other third parties via email without agreement.

5.18 Students are made aware that all email messages are monitored and that the filtering system will detect inappropriate links, viruses, malware and profanity.

5.19 All staff and student email messages are monitored.

5.20 Spam filters will be used to detect spam emails.

5.21 The Ethos Activities will, each year, explaining what a phishing email might look like - including information on the following:

- Determining whether or not an email address is legitimate
- Knowing the types of address a phishing email could use
- Asking 'does it urge the recipient to act immediately?'
- Checking the spelling and grammar.

5.22 Staff will not be punished if they are caught out by cyber attacks as this may prevent similar reports in the future. The ICT team will conduct an investigation; however, this will be to identify the cause of the attack, any compromised data and if there are any steps that can be taken in the future to prevent similar attacks happening. Staff will be educated with preventative measures for the future.

Social Networking:

5.23 The use of social media on behalf of the school will be conducted following the processes outlined in our **Social Media Policy**.

5.24 Access to social networking sites will be filtered as appropriate.

5.25 Should access be needed to social networking sites for any reason, this will be monitored and controlled by staff at all times and must be first authorised by the Principal.

5.26 Students are regularly educated on the implications of posting personal data online outside of the school.

5.27 Staff are regularly educated on posting inappropriate photos or information online, which may potentially affect their position and the school as a whole.

5.28 Staff are not permitted to communicate with students over social networking sites and are reminded to alter their privacy settings.

5.29 Staff are not permitted to publish comments about the school which may affect its reputation.

5.30 Staff are not permitted to access social media sites during teaching hours unless it is beneficial to the material being taught.

Published Content on the School Website:
The school website will meet all statutory requirements and guidelines as required by the DfE and the school website will be audited annually on behalf of the Governors to ensure it is fully compliant with this policy and this will be reported to the Governing Board.

5.31 The Principal will be responsible for the overall content of the website and will ensure the content is appropriate and accurate.

5.32 Contact details on the school website will include the phone number, email and address of the school - no personal details of staff or students will be published.

5.33 Images and full names of students, or any content that may easily identify a student, will be selected carefully and will not be posted until authorisation from parents has been received.

5.34 Students are not permitted to take or publish photos of others without permission from the individual.

5.35 Staff are able to take pictures, though they must do so in accordance with our **Photography Policy**. Staff will not take pictures of students using their personal equipment.

5.36 Any member of staff that is representing the school online, for example through blogging, must express neutral opinions and not disclose any confidential information regarding the school, or any information that may affect its reputability.

Mobile Devices and Laptops:

5.37 The school promotes a sensible usage policy on mobile phones. Use is discouraged in school buildings and prohibited in lessons unless an educational need.

5.38 Students are not permitted to access the school's Wi-Fi system at any time using their mobile devices and hand-held computers. Sixth Form students are permitted to use the school's Wi-Fi system in appropriate places.

5.39 Staff are permitted to use hand-held computers which have been provided by the school, though internet access will be monitored for any inappropriate use by the ICT team where it is justifiable to do so and the justification outweighs the need for privacy.

5.40 The sending of inappropriate messages or images from mobile devices is prohibited.

5.41 Mobile devices will not be used to take images or videos of students and staff.

5.42 No mobile device or laptop owned by the school will be used to access public Wi-Fi networks. ICT technicians will inform students and staff members of this rule before they can use school-owned devices away from the premises.

5.43 The ICT technicians will, in collaboration with the E-Safety Officer, ensure all school-owned devices are password protected.

5.44 To protect, retrieve and erase personal data, all mobile devices and laptops in school are school fitted with software to ensure they can be remotely accessed on-line.

5.45 ICT technicians will review all mobile devices and laptops owned by the school on a regular basis. The MDM (Mobile Device Management) that is in place restricts the addition of apps.

5.46 ICT technicians and the E-Safety Officer will review and authorise any apps and/or computer programmes before they are downloaded - no apps or programmes will be installed without express permission from an ICT technician.

5.47 Apps will only be downloaded from manufacturer approved stores, for example Google Play and the Apple App Store.

Network Security:

5.48 Network profiles for each student and staff member are created in which the individual must enter a username and personal password when accessing the ICT systems within the school.

5.49 Passwords have a minimum length, to prevent 'easy passwords or mistakes when creating passwords.

5.50 Passwords will require a mixture of letters, numbers to ensure they are as secure as possible.

5.51 Passwords will expire after **90** days to ensure maximum security for student and staff accounts.

5.52 Passwords should be stored using non-reversible encryption.

5.53 The E-Safety officer and ICT technicians will ensure all school-owned laptops and computers have their encryption settings turned on or, if there is no built-in encryption option, encryption software is installed.

5.54 Important folders, for example those including students' medical records will be password protected to ensure their security - the E-Safety Officer, Student Welfare Officer and other designated individual(s) will be the only people who have access to this password.

Virus Management

5.55 Technical security features, such as virus software, are kept up-to-date and managed by the E-Safety Officer.

5.56 The E-Safety Officer will ensure that the filtering of websites and downloads is up-to-date and monitored.

5.57 Firewalls will be switched on at all times - ICT technicians will review these on a weekly basis to ensure they are running correctly and to carry out any require updates.

5.58 Firewalls and other virus management systems, for example anti-virus software, will be maintained in accordance with the school's **Data Security Breach Prevention and Management Plan**.

5.59 Staff members will report all malware, ransomware and virus attacks to the ICT technicians and Data Protection Officer (DPO) immediately.

6. CYBER BULLYING

6.1 For the purposes of this policy, cyber bullying is a form of bullying whereby an individual is the victim of harmful or offensive messages, or the posting of information or images online.

6.2 The school recognises that both staff and students may experience cyber bullying and is committed to responding appropriately to instances that should occur.

6.3 The school will regularly educate staff, students and parents on the importance of staying safe online, as well as being considerate to what they post online.

6.4 Students will be educated about online safety through teaching and learning opportunities as part of a broad and balanced curriculum; this includes covering relevant issues within PSHE lessons as well as sex and relationship education.

6.5 The school will commit to creating a learning and teaching environment which is free from harassment and bullying, ensuring the happiness of all members of staff and students.

6.6 The school has zero tolerance for cyber bullying, and any incidents will be treated with the utmost seriousness and will be dealt with in accordance with our **Anti-Bullying Policy**.

6.7 The Principal will decide whether it is appropriate to notify the police or the action taken against a student.

7. REPORTING MISUSE

7.1 Thorpe St Andrew School and Sixth Form will clearly define what is classed as inappropriate behaviour in the **Acceptable Use Agreement**, ensuring all students and staff members are aware of what behaviour is expected of them.

7.2 Inappropriate activities are discussed and the reasoning behind prohibiting activities due to E-Safety are explained to students as part of the curriculum in order to promote responsible internet use.

Misuse by Students:

7.3 Teachers have the power to discipline students who engage in misbehaviour with regards to internet use. All incidents of inappropriate internet use will be recorded on CPOMS.

7.4 Any instances of misuse should be immediately reported on CPOMS.

7.5 Any student who does not adhere to the rules outlined in our **Acceptable Use Agreement** and is found to be wilfully misusing the internet will receive consequences in line with the **Behaviour for Learning** policy.

7.6 Complaints of a child protection nature, such as when a student is found to be accessing extremist material, shall be dealt with in accordance with our **Whole School Policy for Safeguarding Incorporating Child Protection**.

Misuse by Staff:

7.7 Any misuse of the internet by a member of staff should be immediately reported to the Principal, using email.

7.8 The Principal will deal with such incidents in accordance with the **Allegations of Abuse Against Staff Policy** and may decide to take disciplinary action against the member of staff.

7.9 The Principal will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of the action taken against a member of staff.

Use of Illegal Material:

7.10 In the event that illegal material is found on the school's network, or evidence suggests that illegal material has been accessed, the police will be contacted.

7.11 Incidents will be immediately reported to the Internet Watch Foundation and the police will be contacted if the illegal material is, or is suspected to be, a child sexual abuse image hosted anywhere in the world, a non-photographic child sexual abuse image hosted in the UK, or criminally obscene adult content hosted in the UK.

7.12 If a child protection incident is suspected, the school's child protection procedure will be followed - the Designated Safeguarding Lead (DSL) and Principal will be informed and the police contacted.

7.13 Staff will not view or forward illegal images of a child. If they are made aware of such an image, they will contact the DSL.

8. MONITORING AND REVIEW

8.1 This policy will also be reviewed on an **annual** basis by the **Governing Board**; any changes made to this policy will be communicated to all members of staff.

8.2 Members of staff are required to familiarise themselves with this policy as part of their induction programmes.