Online Safety Policy

Date of Policy	September 2020
Review Date	July 2022
SLT Link	Headteacher
Governing Body Link	Chair of Governors

Signature

Date: Sept 2020

Headteacher

Signature

Date:

Chair of Governors

Contents

1. School Vision and Ethos

Our Christian values are at the heart of the ethos of the school and through these we grow individually and as a community. The Story of the Good Samaritan underpins our 7 core values of:

- Honesty
- Forgiveness
- Empathy
- Courage
- Resilience
- Kindness
- Respect.

As a school we have a determination "*to be exceptional in all that we do"* and have an unrelenting commitment to provide:

- Exceptional learning experiences within an environment where students can thrive and learn.
- A caring community that provides students with first class advice, support and guidance, where Children are valued for their individuality and their potential is nurtured and developed.
- A wide range of opportunities that help develop exceptional children with the skills, confidence and knowledge to make a positive contribution to the local and global community both now and in their future lives.

Staff with an exceptional place to work, develop and inspire children

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for Headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is Dan Palmer, Safeguarding Governor

All governors will:

- Ensure that they have read and understand this policy.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendices)

3.2 The Headteacher

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

Details of the school's DSL and Deputy are set out in our child protection and safeguarding policy as well relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Senior Leadership Team, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy (see appendices)
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Senior Leadership Team and/or governing board

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged on MyConcerns and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (see appendices), and ensuring that pupils follow the school's terms on acceptable use (appendices)
- Working with the DSL to ensure that any online safety incidents are logged (on MyConcerns) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet - Childnet International

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

- Relationships and sex education and health education in secondary schools

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

*By the **end of secondary school**, they will know:*

- *Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online*
- *About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online*
- *Not to provide material to others that they would not want shared further and not to share personal material which is sent to them*
- *What to do and where to get support to report material or manage issues online*
- *The impact of viewing harmful content*
- *That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners*
- *That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail*
- *How information and data is generated, collected, shared and used online*
- *How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours*

All schools - adapt this to reflect your school's approach:

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website or virtual learning environment (VLE). This policy will also be shared with parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim. Further details of how the school deals with all forms of bullying including cyberbullying can be found in the Anti-Bullying Policy and Behaviour Policy.

The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Tutors and Heads of Key Stage will discuss cyber-bullying with their tutor groups and year groups, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training (see section 11 for more detail).

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the Anti-Bullying Policy and the Behaviour Policy. Where illegal, inappropriate or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or

- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

8. Pupils using mobile devices in school

Any use of mobile devices in school by students must be in line with the acceptable use agreement (see appendix 1).

In addition details of the rules governing bringing and using mobile phones in school is laid out in the Behaviour Policy.

Any breach of the above agreement or policy may trigger disciplinary action in line with the school Behaviour Policy, which may result in the confiscation of their device.

9. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT Systems Manager.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL and deputy will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be produced via MyConcerns.

This policy will be reviewed annually by the DSL. At every review, the policy will be shared with the governing board.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Anti-Bullying Policy
- Search Policy
- Privacy Policy
- Cookie Policy
- Site Policy
- Staff Code of Conduct
- Staff Disciplinary Procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

Appendix 1: Acceptable Use of ICT and the Internet

Acceptable use of ICT and the Internet

The use of ICT (Information and Communications Technology) hardware and software is a major feature in teaching and learning throughout the school curriculum, and also extends to use at home. A large amount of school resources is committed to ICT and is an area in which students are expected to exercise care and respect of hardware, and the time invested in ensuring systems and software work well for all the school community.

As students use ICT to develop projects and coursework they are very much dependent on the responsible use of ICT equipment by their peers. We would like students to agree to a code of conduct that ensures that opportunities to work on our computers, and the actual work developed by fellow students, are fully respected. Before being allowed to use the school systems both the student and yourself must sign and return the ICT Agreement Form as evidence of your approval, their acceptance of the school rules on this matter, and the use of school computer systems in general.

All students will receive E-Safety, Cyber Bullying and Social Network awareness lessons and presentations through their time at Sexey's School. Access to the Internet will enable students to explore thousands of libraries, databases, and communicate with other Internet users throughout the world. Families should be warned that some material accessible via the Internet may contain items that are illegal, defamatory, inaccurate or potentially offensive to some people. We will protect students as far as possible from unsuitable and unacceptable content by using an Internet Watch Foundation (IWF) approved filtering system and by managing the time during which an internet connection is available to students depending on their age.

Whilst our aim for Internet use is to further educational goals and objectives, students may find ways to access inappropriate other materials as well. We believe that the benefits to student from access to the Internet, in the form of information resources and opportunities for collaboration, exceed any disadvantages. However ultimately, parents and guardians of students are responsible for setting and conveying the standards that their children should follow when using media and information sources. To that end, the school supports and respects each family's right to decide whether or not to apply for access.

Year 10 and above: The use of personal mobile devices in school is generally reserved for students in year 10 and above, unless there are special educational requirements that have been pre agreed. Should you provide your child with a device (phone/tablet/laptop) for their personal use, it must never be connected to the main school network. The school has a site wide student Wi-Fi to which students may be permitted access for their own devices, it should be noted that this connection is filtered at all times and all activity is logged to the specific users. Any misuse will result in the user losing their access rights to it. The use of alternative unfiltered internet connections (e.g. 4G) is seriously discouraged.

Boarding Pupils: The school Wi-Fi extends to all boarding houses and all boarding pupils will be permitted access for their own devices. In addition to the normal filtering and logging on the system, access to use the internet is restricted in evenings and at weekends by time limits specific to age group. It should be noted that some social media sites and apps are restricted due to their own recommended minimum age limits. If parents provide an alternative unfiltered internet connection (4G) on phones or tablets, then they take full responsibility for the use and potential misuse of it by their child.

Microsoft Office 365 is used at Sexey's which allows for the installation of MS Office on up to 5 personally owned PCs/Macs. Microsoft Office 365 is provided on a subscription basis - students can

use the latest version of Office whilst registered with the School and have an active school user account. The account will only remain active for 30 days after leaving school, although this will be extended for 2 weeks after exam results day for year 11 and 13 pupils.

We would be grateful if you could read the enclosed guidance document and rules for the use of personal mobile devices, then complete and return the ICT agreement form.

Yours faithfully

ICT Systems Manager

RULES FOR THE USE OF PERSONAL DEVICES WITHIN SCHOOL

If students have been given permission to bring their own mobile devices to use in school, the rules for the use of these devices during the school day and in the boarding houses (if applicable) are laid down below and must be adhered to.

1. All students bringing a mobile device into school are to provide are to ensure the power supply is safe to use at all times.
2. The owner of the mobile device is wholly responsible for the actions of any other user who they permit to use it.
3. Pornographic, indecent or images likely to offend others are never to be shown or saved on the mobile device.
4. There is a Wi-Fi network available within school and the boarding houses and details of how to connect will be provided to all boarding students during the first week of term. The mobile device must NEVER be connected to the main school network.
5. All Windows mobile devices are to have anti-virus software installed and kept up-to-date.
6. The school will generally not provide any software for personal mobile devices. (see note below)
7. Users are responsible for ensuring that any important work is backed up regularly, or transferred to the school network, where nightly backups are taken.
8. Users are to allow unrestricted access to all files and folders on the mobile device to any member of the IT staff should they be requested and required to do so.
9. The user is totally responsible for maintaining the mobile device and although technical advice and help may be given by the IT department, no liability can be accepted if that advice proves to be incorrect.
10. The school accept no responsibility for the security of the mobile device at any time.
11. The use of mobile devices in school is subject to a separate policy and rules.
12. Power leads are not to be trailed across any walking space.

Note:

Microsoft Office 365 is used at Sexey's which allows for the installation of MS Office on up to 5 personally owned PCs/Macs.

Microsoft Office 365 is provided on a subscription basis - students can use the latest version of Office whilst registered with the School and have an active school user account. The account will only remain active for 30 days from leaving school.

Appendix 2: permission and agreement forms

ACCEPTABLE USE OF ICT AND THE INTERNET - PARENT PERMISSION FORM

Student

As a school user of the Internet, I agree to comply with the school rules on its use. I will use the Internet Access provided by the school in a responsible way, and observe all the restrictions explained to me by the school.

I also undertake to abide by school rules concerning the acceptable use of ICT resources, and respect the work and privacy of other students and staff.

If I use a personal mobile device within school, I agree to abide to the rules for the use of personal mobile devices and to provide any details requested and permit access to all files on it, if required.

The mobile device **must not** be connected to the main school network at any time.

Student Name _____ Student Signature _____Date: ___/___/___

Parent

As the parent or legal guardian of the student signing above, I grant permission for my son/daughter to use electronic mail and the Internet. I understand that students will be held accountable for their own actions. I also understand that some materials on the Internet may be objectionable and I accept responsibility for setting standards for my son/daughter to follow when selecting, sharing and exploring information and media.

I agree that should my son/daughter bring into school a personal mobile device that it remains the responsibility of the owner, and that any misuse may result in permission to use the mobile device being withdrawn.

Parent Name _____ Parent Signature _____Date: ___/___/___

Acceptable use of ICT and the Internet - Staff

Please complete and return this form to the IT Systems Manager.

As a user of the schools computer systems, I agree to comply with the schools Acceptable Usage Policy (AUP), available on Moodle. I will use the computers, email and Internet provided by the school in a responsible way, and observe all the restrictions explained to me.

I undertake to use the school ICT resources appropriately for teaching and learning and will respect the privacy of other staff and students.

When using the schools system I will ensure I do not compromise the security policies in place, particularly when connected to the network, and will not allow students to use my usernames or passwords at any time.

When using a laptop outside of school I am aware that, as school property, it should not be used in a manner that may reflect inappropriately on the school. I am aware that laptops are NOT encrypted and that pupils personal data should not be stored on them at any time.

I understand that the ICT staff has unrestricted access to all areas of the network and that any laptop or portable storage device may be requested for inspection by SLT/ICT staff at any time and I must provide all necessary details on demand.

Teaching	Admin	PGCE	Boarding	Gap	Supply	Visitor
☐	☐	☐	☐	☐	☐	☐

Staff Name: _____

Staff Signature: _____

Date: _____

Acceptable use of ICT and the Internet: Governors and Guests

Please complete and return this form to the ICT Systems Manager.

As a user of the schools computer systems, I agree to comply with the schools Acceptable Usage Policy (AUP). I will use the computers, email and Internet provided by the school in a responsible way, and observe all the restrictions explained to me.

I undertake to use the school ICT resources appropriately and will respect the privacy of other staff and students.

When using the schools system I will ensure I do not compromise the security policies in place, particularly when connected to the network, and will not unauthorized persons to use my usernames or passwords at any time.

I understand that the ICT staff have unrestricted access to all areas of the network and that any laptop or portable storage device may be requested for inspection by ICT staff at any time and I must provide all necessary details on demand.

Name (Please Print Clearly) _____

Signature_____

Date: ___/___/___

Appendix 3: ICT use guidelines for parents

SEXEY'S SCHOOL ICT USE GUIDELINES FOR PARENTS

Every attempt should be made for staff, parents and students to work together so that use of the internet is as safe as possible. All equipment and other users should be treated with respect and the facilities should be used in a way that does not disrupt its use by others.

This means that:

- Users should take responsibility for their personal access facilities. They should not allow others access to their user IDs or email accounts and all passwords should be kept private and changed regularly
- no attempt should be made to bypass security or gain access to another user's account
- email addresses should only be passed to trusted individuals
- any email from unknown sources should be deleted immediately
- users should be made aware that inappropriate e-mail sent by them may be recorded and may be traced back to them
- any person who believes that attempts have been made to make unacceptable use of the internet should report the matter immediately to a member of staff
- any person who discovers any materials they consider may be offensive or inappropriate should report the matter immediately to a member of staff
- any material published on the Web or through other electronic means should not contain any offensive material and should be checked by a member of staff before being made publicly available
- users should not use their home address or phone number or those of other students or when on the network
- users should be aware that internet access is monitored and that every site they attempt to visit is recorded and may be traced back to them
- the school reserves the right to restrict or remove access in the event of any user misusing network and communication facilities.

As well as these, a number of aspects are under the strict control of the classroom teacher.

- The use of chat and newsgroups is restricted. Any use of these facilities should be in line with specific instructions issued by the class teacher.
- Saving or downloading materials is subject to guidance from the class teacher. Materials saved or downloaded from the internet must not infringe copyright.
- Students must ensure that any form of removable data is virus free before using it.

Appendix 4: online safety training needs – self audit for staff

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a student approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for students and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	

Appendix 5: Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.