KING EDWARD VI
SHELDON HEATH ACADEMY

E-Safety Policy

This policy was adopted by
the Curriculum & Student Welfare Committee
on 10th June 2021
Next review due summer 2022, or earlier if the need arises

CONTENTS

1. AIMS

The 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 the School Trust 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 statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and 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.

This policy complies with our funding agreement and articles of association.

3. ROLES AND RESPONSIBILITIES

3.1 The Trustee Board and Local Governing Body

The Trustee Board has overall responsibility for monitoring this policy and holding the principal to account for its implementation.

The Local Governing Body 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).

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 (appendix 2a and 2b)
-

3.2 The principal

The principal 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 designated safeguarding lead (DSL) and any deputies are set out in our child protection and safeguarding policy.

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

- Supporting the principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the school

- Working with the principal, ICT Technical Team and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged via our smoothwall and CPOMS system and that these are dealt with appropriately in line with this policy
- 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
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the principal and Local Governing Body

This list is not intended to be exhaustive.

3.4 The ICT Technical Team

The ICT Technical Team 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 using school networks or hardware, 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 monthly 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 (see appendix 4) 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 (appendix 2a and 2b), and ensuring that pupils follow the school's terms on acceptable use (appendix 1a and 1b)
- Working with the DSL to ensure that any online safety incidents are logged via smoothwall 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 principal 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 (appendix 1a and 1b)

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

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hottopics

Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parentsfactsheet-09-17.pdf

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 (appendix 2). In house AUP

4. EDUCATING PUPILS ABOUT ONLINE SAFETY

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

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

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.

Online safety will also be covered during parents' evenings.

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

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

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 pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Staff will discuss cyber-bullying with their tutor 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 our RSE curriculum, and other subjects where appropriate.

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

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, 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 and 2). In house 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 and 2.

8. PUPILS USING MOBILE DEVICES IN SCHOOL

Pupils may bring mobile devices into school, but are not permitted to use them without express staff consent and supervision.

Sixth form students may use mobile devices within the School after acceptance of and compliance with the BYOD policy (appendix 1b)

Any breach will 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 2a and 2b

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 technical team.

Work devices must be used solely for work activities.

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 the 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, ebulletins and staff meetings).

The DSL and any deputies 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. Incident logs are generated automatically vis Smoothwall and stored in our CPOMS archive.

This policy will be reviewed annually by the Principal At every review, the policy will be shared with the Local Governing Body.

13. LINKS WITH OTHER POLICIES

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices

Complaints procedures

Appendix 1a

Student use of computers, the internet and email

To gain access to the internet and email, all students must obtain parental permission as confirmed below.

The School recognises the value and encourages the use of computers, the internet and email. We also believe that students must be taught to develop the appropriate skills to analyse and evaluate such resources. These skills are a fundamental requirement in the society that our students are entering. Students are therefore taught a code of behaviour for the use of ICT. They are expected to:

- Use all equipment carefully and sensibly making sure that it is not used to harm other people or their work
- Not share passwords with other people
- Only log on to the network/learning platform using my own username and password
- Respect the work of others
- Not access inappropriate or offensive materials
- Not knowingly introduce a virus or malicious software onto the network
- Not use the School network to access social networking sites
- Report any such sites unwittingly accessed
- Use only acceptable and appropriate language
- Not reveal personal information
- Not plagiarise (copy work and pass it off as their own), but to acknowledge any downloaded material
- Not play non-educational games or access material not directly related to educational purposes
- Not to damage computer equipment in any way

Any student breaking this code may have access rights removed. There may also be other disciplinary action in line with the School's policy on offensive language.

I/we support these guidelines.

Student signature: ____________________________ Date: ____________________

Parent/Carer signature: ______________________ Date: ____________________

Appendix 1b

Sixth Form Students - use of computers, the internet and email

To gain access to the internet and email, all Sixth form students must sign this agreement.

The School recognises the value and encourages the use of computers, the internet and email. We also believe that students must be taught to develop the appropriate skills to analyse and evaluate such resources. These skills are a fundamental requirement in the society that our students are entering. Students are therefore taught a code of behaviour for the use of ICT. They are expected to:

- Use all equipment carefully and sensibly making sure that it is not used to harm other people or their work
- Not share passwords with other people
- Only log on to the School network/learning platform using my own username and password
- Respect the work of others
- Not access inappropriate or offensive materials
- Not knowingly introduce a virus or malicious software onto the network
- Not use the School network to access social networking sites
- Report any such sites unwittingly accessed
- Use only acceptable and appropriate language
- Not reveal personal information
- Not plagiarise (copy work and pass it off as their own), but to acknowledge any downloaded material
- Not play non-educational games or access material not directly related to educational purposes
- Not to damage computer equipment in any way

Any student breaking this code may have access rights removed. There may also be other disciplinary action in line with the School's policy on offensive language.

I support these guidelines.

Student Signature: ______________________ Date: ________________________

Appendix 2a

Staff Agreement on the Use of ICT Internet Policy

King Edward VI Sheldon Heath School recognises the value of, and encourages the use of, the rich information sources available on the Internet. The School understands that use of the Internet is beneficial for preparing for interesting stimulating lessons and for good educational management.

Staff Agreement

I have read the ICT Policy and I understand that I am responsible for the use of the Internet and my network account, under my user name. Staff should, through their best endeavours, refrain from the following

- Accessing any sources that would be considered illegal or exhibit inappropriate/offensive materials.
- Revealing personal images or information of oneself or others.
- Accept responsibility not to download copyrighted material i.e. software, games, music, graphics, videos or text materials that are copyright.
- Sending or displaying offensive messages or pictures.
- Using obscene language.
- Harassing, insulting or attacking others.
- Intentionally damaging or altering settings on computers, computer systems or computer networks.
- Intentionally violating copyright laws.
- Using others' passwords.
- Opening other people's folders, work or files.
- Use of personal email addresses to communicate with students.

The School does not accept responsibility for backing up files stored locally on a portable work device, such as a laptop or tablet. Staff are therefore encourage to use the School's remote access solution on their work devices to log onto the network. This means all files will be backed up and stored securely on the network.

Additionally for data security, no student data should be stored locally on work devices, for instance tracking sheets. Any such files should be accessed through the School's remote access solution, where they are securely stored.

Staff are encouraged to share any concerns with the ICT support team and seek their advice and counsel at any point. If in doubt check first!

All use of the School's system is monitored. Should any inappropriate usage become apparent, this will be drawn to the attention of a senior colleague and may result, if appropriate, in further action.

As a user of the Internet, I agree to comply with the above policy on Internet use. I will use computers and the network in a responsible and professional manner and observe all the rules explained to me by the School.

Staff signature: ___________________________

Print name: _______________________________

Date: ____________________________________

This form should be returned to Human Resources to ensure access to appropriate systems.

Appendix 2b

Safer Practice with Social Networking Sites

Social networking is a way of life for most young people and many adults, however, adults working with children and young people must review their use of social networks as they take on professional responsibilities. This is particularly important with services such as FaceBook where boundaries between personal life and professional role sometimes blur.

The School's Safeguarding Guidance booklet –'Guidance for Safer Working Practice for Adults who Work with Children and Young People' published by Government Office North West Jan 2009 states on page 16.

"...... Communication between adults and children, by whatever method, should only take place within clear and explicit boundaries. This includes the wider use of technology such as mobile phones, chat rooms, text messaging, emails, digital cameras, web-cams, websites and blogs. Adults should not share any personal information with the child or young person. They should not request, or respond to, any personal information from the child/young person, other than that which might be appropriate as part of their professional role. Adults should ensure that all communications are transparent and open to scrutiny."

Adults should:

- Not give their personal contact details to children or young people, including their mobile telephone number and details of any blogs or personal websites.
- Only use equipment e.g. mobile phones, provided by the organisation to communicate with children, making sure that parents have given permission for this form of communication to be used.
- Only make contact with children for professional reasons and in accordance with any organisation policy.
- Recognise that text messaging is rarely an appropriate response to a child in a crisis situation or at risk of harm. It should only be used as a last resort when other forms of communication are not possible.
- Not use internet or web-based communication channels to send personal messages to a child/young person.
- Ensure that if a social networking site is used, details are not shared with children and young people and privacy settings are set at maximum.

The School's policy is that staff must not communicate with any current students including 6th form students or ex-students under the age of 18 via social networking sites (other than sites set up by the School and then only within the professional boundaries indicated above). Staff must not accept these young people as 'friends' on social networking sites and must delete any of these young people currently accepted as 'friends' on their social networking sites.

All teaching, non-teaching staff and volunteers are required to:

- Check carefully the credentials of anybody who asks to be your ‘friend’. With most sites you can see who a person is connected to before connecting to them yourself. If you don’t know any of their friends, you can always phone the person they seem to be or wait for them to contact you again through another channel. Review ‘friends lists’ regularly and remove any current student or person under the age of 18 years where it could be perceived as inappropriate to maintain contact with that young person. Do not put yourself in a position of vulnerability whereby your motivation and intentions can be questioned.
- Check the content of your profile regularly including checking there are no inappropriate comments or photographs displayed. With systems such as FaceBook, your ‘friends’ can post undesirable material on your profile without your authorisation. If you have been tagged on photographs with students, ensure these are removed immediately.
- Avoid publishing material about your place of work as it is too easy for it to be passed on and taken out of context. Posting comments, photographs or suggestions on such sites that could bring the School into disrepute will be considered under the appropriate Disciplinary Policy.
- Use a strong password for any social networking system. Use numbers as well as upper and lower case letters.
- Ensure your profile is set to be ‘secure’ or ‘private’ so that only people you accept as ‘friends’ can view it. This prevents children, young people and their families from accessing your personal information.
- With the maximum security settings applied, your ‘friends’ list cannot be viewed by those trying to access your profile. However, if you do not apply the maximum setting, the profiles of your friends with low security settings can be viewed, which in turn means that any material you have posted, or anyone else has posted about you on your ‘friends’ profile can be seen. This includes any photos in which they have ‘tagged’ you. To set security settings to your FaceBook profile, go to ‘settings’ and then ‘Privacy Settings’.

Should any member of staff be found not adhering to this policy, action will be considered under the School’s Disciplinary and Dismissal policy.

Please sign below to indicate your receipt and understanding of and compliance with this policy.

I…………………………….. (Name) acknowledge receipt and understanding of the

School’s Safer Practice with Social Networking Sites Policy

Signature:………………………………………………… Date:…………………………….