E-Safety

December 2021

The Internet Policy relates to other policies including those for ICT, GDPR, Safeguarding, Safe Practice Policies, behaviour including Anti Bullying Policy and for Personal development. Staff, parents, Academy Councillor and pupils have been consulted in deciding the policy.

This policy has been written by the school, building on the Staffordshire LA policy and government guidance. It has been agreed by the senior leadership team and approved by Academy Councillors. It will be reviewed annually.

Rationale

New technologies have become integral to the lives of young people in today's society, both within the School and in their lives outside school. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

The requirement to ensure that young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in the School are bound. An E-Safety Policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the Principal and Academy Council to the Leadership Team and classroom teachers, support staff, volunteers, parents/carers, members of the community and the students themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote student achievement. However, the use of these new technologies can put young people at risk within and outside the School. Good education provision, to build students' resilience to the risks to which they may be exposed, will allow students the confidence and skills to face and deal with these risks.

The School must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The E-Safety Policy that follows explains how the School intends to do this, while also addressing wider educational issues in order to help young people (and their parents/carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Development/Monitoring/Review of this Policy

Scope of the Policy

This Policy applies to all members of the School community (including staff, students, volunteers, parents/carers, visitors, community users) who have access to and are users of School ICT systems, both in and out of School.

The Teaching Online Safety In school June 2019 **DfE external document template (publishing.service.gov.uk)** is to keep people safe online, support for parents and carers, developing children's digital literacy. to support and act on the behaviour of students when they are off the School site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the School.

The School will deal with such incidents within this Policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

Principal and Leadership Team:

- The Principal is responsible for ensuring the safety (including e-safety) of members of the School community, though day to day responsibility for e-safety will be delegated to the Designated Safeguarding Lead and Lead E-Safety Teacher.

- The Principal/Lead E-Safety Teacher/Designated Safeguarding Lead are responsible for ensuring that relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

- The Principal, Vice Principal, Lead E-Safety Teacher and Designated Safeguarding Lead should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

Network Manager:

The Network Manager is responsible for ensuring:

- that the School's ICT infrastructure is secure and is not open to misuse or malicious attack;
- that the School meets the e-safety technical requirements outlined in any relevant Local Authority E-Safety Policy and guidance;
- that users may only access the School's networks through a properly enforced password protection policy, in which passwords are regularly changed;
- the school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person;
- that they keep up-to-date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant;
- that the use of the Network, remote access, email is regularly monitored in order that any misuse or attempted misuse can be reported to the Lead E-Safety Teacher and Principal;
- that monitoring software/systems are implemented and updated as agreed in School policies.

Teaching and Support Staff:

Teaching and Support Staff are responsible for ensuring that:

- they have an up-to-date awareness of e-safety matters and of the current School E-Safety Policy and practices;
- they have read, understood and signed the School ICT Acceptable Use Policy/Agreement;
- they report any suspected misuse or problem to the E-Safety Lead Teacher and Principal;
- digital communications with students (e.g. email/ class charts) should be on a professional level and only carried out using official School systems;
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current School policies with regard to these devices.

Designated Person for Safeguarding:

Should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data;
- access to illegal/inappropriate materials;
- inappropriate on-line contact with adults/strangers;
- potential or actual incidents of grooming;
- cyber-bullying.

Students:

- are responsible for using the School ICT systems in accordance with the Student Acceptable Use Policy, which they will be expected to sign before being given access to School systems;
- should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright

regulations;

- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- will be expected to know and understand School policies on the use of mobile phones, digital cameras and hand-held devices, they should also know and understand School policies on the taking/use of images and on cyber-bulling;
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the School's E-Safety Policy covers their actions out of school, if related to their membership of the School.

Parents/Carers:

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The School will, therefore, take every opportunity to help parents understand these issues through a range of mediums. These could include; parents' evenings, newsletters, letters, website and information about national/local e-safety campaigns. Parents/ carers have a responsibility to monitor their child's usage and content they watch or post on their child's own personal devices and any devices used outside of school.

Academy Council:

The Academy Council is responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the Policy.

Use of digital and video images – Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The School will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet, e.g., on social networking sites.
- Staff are allowed to take digital/video images to support educational aims, but must follow School policies concerning the sharing, distribution and publication of those images.
- Care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the School into disrepute.
- Students must not take, use, share publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere, that include students will comply with GDPR guidance and good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the School website.
- Students' work can only be published with the permission of the student and parents or carers.

Data Protection
Personal data will be recorded, processed, transferred and made available according to the GDPR (2018) which states that personal data must be:

- Lawfully processed, transparent and for a specified purpose
- Processed for limited purposes and will be deleted afterwards
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure.
- Only transferred to others with adequate protection

Staff must ensure they:

- Follow the GDPR guidelines
  - At all times take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse.
  - Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
  - No personal data is stored on any portable computer system, USB stick or any other removable media.
  - Transfer data using encryption and secure password protected devices.

Communications
A wide range of rapidly developing communications technologies has the potential to enhance learning.
When using communication technologies, the School considers the following as good practice:

- The official School email service may be regarded as safe and secure and is monitored.
- Users must immediately report to the Line Manager/ SLT/ Designated safeguarding Lead in accordance with School policy, the receipt of any email that makes them feel uncomfortable is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students or parents/carers (email, school text service, etc.) must be professional in tone and content. These communications may only take place on official (monitored) School systems. Personal email addresses, text messaging, or public chat/social networking programmes must not be used for these communications.
- Personal information should not be posted on the School website and only official email addresses should be used to identify members of staff.

Unsuitable/inappropriate activities
Some internet activity, eg, accessing child abuse images or distributing racist material, is illegal and would obviously be banned from School and all other ICT systems. Other activities, eg, cyberbullying, would be banned and could lead to criminal prosecution. There are, however, a range of activities which may, generally, be legal, but would be inappropriate in a School context, either because of the age of the users or the nature of those activities.

1 Why is Internet use important?

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.
- Internet access is an entitlement for pupils who show a responsible and mature approach to its use.

2 How does the Internet benefit education?

- Access to world-wide educational resources including museums and art galleries;
- Inclusion in government initiatives
- Educational and cultural exchanges between pupils world-wide;
- Cultural, vocational, social and leisure use in libraries, clubs and at home;
- Access to experts in many fields for pupils and staff;
- Staff professional development through access to national developments, educational materials and good curriculum practice;
- Communication with support services, professional associations and colleagues; improved access to technical support including remote management of networks;
- Exchange of curriculum and administration data with the LA and DFE.

3 How will Internet use enhance learning?

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- All pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

4 How will pupils learn to evaluate Internet content?

- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Designated or deputy designated leads (Mr L Hope, Mrs Snape, Miss Boustead, Mrs Skelding) in the first instance.
- Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

5 How will e-mail be managed?

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal details of themselves or others in e-mail communication, such as address or telephone number, or arrange to meet anyone.
- Access in school to external personal e-mail accounts may be blocked.
- Excessive social e-mail use can interfere with learning and will be restricted.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

6 How will Web site content be managed?

- The point of contact on the Web site should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- Web site photographs that include pupils will be selected carefully.

- Pupils’ full names will not be used anywhere on the Web site, particularly in association with photographs.
- Permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- The Principal or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The Web site should comply with the school's guidelines for publications.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

7 Use of newsgroups

- Newsgroups will not be made available to pupils unless an educational requirement for their use has been demonstrated.

8 Can Social Networking be made safe?

- Pupils will not be allowed access to public or unregulated social networking sites.
- Pupils should only use school e-mail to communicate with each other and their teachers. This use will be supervised and the importance of e-safety emphasised.
- Staff should only use school e-mail to communicate with pupils.
- A risk assessment will be carried out before pupils are allowed to use a new social networking technology in school.
- Social network use by pupils outside of the school will be monitored by parents and carers

9 How will emerging technologies be managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Pupils should not use mobile phones during lessons or formal school time except at lunchtime in the designated area
- The sending of abusive or inappropriate messages is forbidden.

10 How will Internet access be authorised?

- The school will keep an electronic record of any pupils whose parents have specifically requested that they should be denied internet or e-mail access.
- All pupils will be provided with supervised Internet access
- Parents and pupils will be asked to sign the Acceptable Use document.

11 How will the risks be assessed?

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor the LA can accept liability for the material accessed, or any consequences of Internet access.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The Principal will ensure that the E-Safety policy is implemented and compliance with the policy monitored.

12 How will filtering be managed?

- The school will work in partnership with parents; the LA, DFE, the Internet Service Provider and Shaw Education Trust to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the designated safeguarding lead, Mr L Hope or the Deputy Safeguarding Leads, Mrs Snape, Miss Boustead or Mrs Skelding.
- The Safeguarding Lead will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Filtering strategies and appropriate software will be selected by the Shaw Education Trust. The filtering strategy will be selected to suit the age and curriculum requirements of the pupils.

13 How will the policy be introduced to pupils?

- Rules for Internet access will be posted in all rooms where computers are used.
- Pupils will be informed that Internet use will be monitored.
- Instruction in responsible and safe use should precede Internet access.
- Pupils will be reminded of the rules and risks at the beginning of any lesson using the Internet
- A module on responsible Internet use will be included in the Personal development programme covering both school and home use.
- Regular assemblies will be held for all year groups on the theme of e-safety.

14 How will staff be consulted?

- All staff required to work within the terms of the school 'Acceptable Use Policy'.
- All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the 'Acceptable Use Policy' on joining the school and its importance will be explained to them.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- The monitoring of Internet use is a sensitive matter. The Safeguarding Lead monitors use on a regular basis through a software package.
- Staff development training in E-Safety and on the school 'Acceptable Use Policy' will be provided as required.

15 How will ICT system security be maintained?

- The school ICT systems are reviewed regularly with regard to security.
- Virus protection is installed and updated regularly.
- Security strategies are discussed with the Shaw Education Trust, particularly where a wide area network connection is being planned.
- Personal data sent over the Internet will be encrypted or otherwise secured.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.
- Files held on the school's network will be regularly checked.
- The Network Manager will ensure that the system has the capacity to take increased traffic caused by Internet use.

16 How will complaints regarding Internet use be handled?

- Responsibility for handling incidents will be delegated to the Principal and Safeguarding Lead.
- Any complaint about staff misuse must be referred to the Principal.
- Pupils and parents will be informed of the complaints procedure.

- Parents and pupils will need to work in partnership with staff to resolve issues.
- As with drugs issues, there may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.
- Sanctions available include:
    - interview/counselling;
    - informing parents or carers;
    - removal of Internet or computer access for a period, which could ultimately prevent access to files held on the system, including examination coursework.

17 How will parents' support be enlisted?

- Parents' attention will be drawn to the 'Acceptable Use Policy' through parent e-safety information.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and information provided for safe Internet use at home.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.
- Interested parents will be referred to organisations such as Child Exploitation and Online Protection (CEOP).

18 How is Internet used across the community?

- Adult users will need to sign the 'ICT Acceptable Use" agreement.
- Parents/carers of pupils will be required to sign the 'Acceptable Use Policy' on behalf of their child.

Policy Review:

Signed by: (Principal) Signed by: (Chair of Academy Council)

Date: 9th December 2021 Next Review Date: December 2024