Broughton Hall High School
Technology College

E-SAFETY POLICY

Who will write and review the policy?

- The school will appoint an e-Safety Coordinator. This may be the Designated Child Protection Coordinator as the roles overlap.
- Our e–Safety Policy has been written by the school, building on the KCC e–Safety Policy and government guidance. It has been agreed by the Senior Leadership Team and approved by governors and the PT.
- When staff, pupils etc. leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.
- Parents will be requested to sign an e–Safety/internet agreement as part of the Home School Agreement in pupil planners.
- The e-Safety Policy and its implementation will be reviewed annually by the Safeguarding Officer and an e-Safety Group.

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 functions.
- Internet use is part of the statutory curriculum and a necessary tool for learning.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- The Internet is a part of everyday life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.

How does Internet use benefit education?

- access to world-wide educational resources including museums and art galleries;
- inclusion in the National Education Network (NEN) which connects all UK schools;
- educational and cultural exchanges between pupils world-wide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across networks of schools, support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- Access to learning wherever and whenever convenient.

- exchange of curriculum and administration data with KCC and DCSF;

How can Internet use enhance learning?

- The schools will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

How will pupils learn how to evaluate Internet content?

- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of on-line materials is a part of teaching/learning in every subject.

How will information systems security be maintained?

- Virus protection will be updated regularly.
- The security of the school information systems and users will be reviewed regularly.
- Unapproved software will not be allowed in pupils' work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The school Internet access will be designed to enhance and extend education.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

How will e-mail be managed?

- Pupils may only use approved e-mail accounts.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Access in school to external personal e-mail accounts may be blocked.
- Excessive social e-mail use can interfere with learning and may be restricted.
- The forwarding of chain messages is not permitted.
- Staff should only use school email accounts to communicate with pupils as approved by the Senior Leadership Team.

How will published content be managed?

- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.
- Email addresses should be published carefully, to avoid being harvested for spam (e.g. replace '@' with 'AT').
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

Can pupil's images or work be published?

- Images that include pupils will be selected carefully and will not provide material that could be reused.

- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Opt out letters to parents or carers will be circulated before images of pupils are electronically published.
- Pupils work can only be published with their permission or their parents/carers.

How will social networking, social media and personal publishing be managed?

- The schools will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
- Pupils should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name or school.
- Teachers' official blogs or wikis should be password protected and run from the school website. Teachers should be advised not to run social network spaces for student use on a personal basis.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.
- Pupils will be educated to use Social media in a safe and efficient way.
- Students should be advised not to publish specific and detailed private thoughts.

How will filtering be managed?

- The school will work with KCC, Becta, LDL and the Schools Broadband team to ensure that systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL must be reported to the e–Safety Coordinator.
- LDL and Mr S Lyon, will manage the configuration of our filtering. This task requires both educational and technical experience.
- Any material that the school believes is illegal must be reported to appropriate agencies such as IWF or CEOP.
- The school's broadband access includes filtering appropriate to the age and maturity of pupils.
- The school's access strategy is designed by educators to suit the age and curriculum requirements of the pupils, with advice from network managers.

How will videoconferencing be managed?

The equipment and network

- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- External IP addresses should not be made available to other sites.
- The equipment must be secure and if necessary locked away when not in use.

- School videoconferencing equipment should not be taken off school premises without permission.

Users

- Parents and carers should opt out if they do not wish their children to take part in videoconferences, in the annual return.
- Responsibility for the use of the videoconferencing equipment outside school time needs to be established with care and supervised by suitably trained personnel.

Content

- Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.
- If third-party materials are to be included, check that recording is acceptable to avoid infringing the third party intellectual property rights.
- Videoconferencing should be supervised appropriately for the pupils' age.
- Establish dialogue with other conference participants before taking part in a videoconference. If it is a non-school site it is important to check that they are delivering material that is appropriate for your class.
- When recording a videoconference lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material shall be stored securely.

How can 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.
- Mobile phones may not be used during lessons or formal school time (as part of the School AUP). The sending of abusive or inappropriate text messages is forbidden.
- The school should investigate wireless, infra-red and Bluetooth communication technologies and decide a policy (as part of the AUP) on phone use in school.
- Staff will be issued with a school phone where contact with pupils is required.

How should personal data be protected?

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

How will Internet access be authorised?

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- All staff must read and sign the **Acceptable Use Policy** before using any school ICT resource – see attached Appendix 1.
- Students must apply for Internet access individually by agreeing to comply with the e-Safety Rules and countersigning their planner.
- Parents will be asked to sign and return a consent form for pupil access.

How will risks be assessed?

- The school should audit ICT use to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate.

- 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 school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot accept liability for the material accessed, or any consequences resulting from Internet use.

How will e-safety complaints be handled?

- Complaints of Internet misuse will be dealt with under the School's Complaints Procedure.
- Any complaint about staff misuse must be referred to the headteacher.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- Discussions will be held with the local Police Safer Schools Partnership Coordinators and/or Children's Safeguards Unit to establish procedures for handling potentially illegal issues.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary and child protection procedures.
- All e–Safety complaints and incidents will be recorded by the school — including any actions taken.

How is the Internet used across the community?

- The school will liaise with local organisations to establish a common approach to e-safety via LDL.
- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

How will Cyberbullying be managed?

- Cyberbullying (along with all forms of bullying) will not be tolerated in school. Full details are set out in the school's policy on anti-bullying.
- There are clear procedures in place to support anyone affected by Cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded.
- There are clear procedures in place to investigate incidents or allegations of Cyberbullying. Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.

How will Learning Platforms and Learning Environments be managed?

- SLT and staff will monitor the usage of the LP by pupils and staff regularly in all areas, in particular message and communication tools and publishing facilities.
- Pupils/staff will be advised on acceptable conduct and use when using the learning platform.
- Only members of the current pupil, parent/carers and staff community will have access to the LP.
- All users will be mindful of copyright issues and will only upload appropriate content onto the LP.
- A visitor may be invited onto the LP by a member of the SLT. In this instance there may be an agreed focus or a limited time slot.
- Pupils may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.

How will the policy be introduced to pupils?

- E-Safety rules will be posted in rooms with Internet access.
- An e–Safety training programme will be introduced to raise the awareness and importance of safe and responsible internet use.
- Pupil instruction in responsible and safe use should precede Internet access.
- An e–Safety module will be included in the PSHE, Citizenship and ICT programmes covering both safe school and home use.
- All users will be informed that network and Internet use will be monitored.
- E–Safety training will be part of the transition programme across the Key Stages and when moving between establishments.
- Safe and responsible use of the internet and technology will be reinforced across the curriculum. Particular attention will be given where pupils are considered to be vulnerable.

How will the policy be discussed with staff?

- The e–Safety Policy will be formally provided to and discussed with all members of staff.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues.
- Staff training in safe and responsible Internet use both professionally and personally will be provided.
- To protect all staff and pupils, the school will implement Acceptable Use Policies.

How will parents' support be enlisted?

- Parents' attention will be drawn to the School e–Safety Policy in newsletters, the school brochure and on the school website.
- Interested parents will be referred to relevant organisations
- A partnership approach with parents will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home Internet use or highlighting e–Safety at other attended events e.g. parent evenings, sports days.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.
- Information and guidance for parents on e–Safety will be made available to parents in a variety of formats.

STAFF ACCEPTABLE USER POLICY

Data Protection

- I understand that I **MUST NOT** disclose any password or login name to anyone, other than the persons responsible for running and maintaining the system.
- I understand that I **MUST NOT** allow any students to use my personal log in to any of the ICT systems for **ANY** reason.
- I understand that I **MUST** take every reasonable precaution to secure any data or equipment removed from the school premises.
- I understand that if I store any data relating to pupils it must be protected by passwords or encryption.
- I understand that equipment taken off site will be my personal responsibility and I am advised to check that its loss or damage is covered by my personal insurance.
- I understand that the School can and will monitor any data on the network to ensure policy compliance, and to aid in resolving networking issues.

Student Protection

- I am aware of all guidelines to conceal student identities when publishing to the public domain.
- I understand that students **MUST** be supervised at **ALL** times when in an ICT suite or on computer equipment.
- When arranging use of ICT facilities I will ensure that a staff member is able to monitor pupils at **ALL** times.
- I have read and understand my role regarding acceptable use and my role in enforcing it.
- I will escalate non-compliance by students in accordance with school policy.
- I understand that I should never give out personal details such as home or mobile phone numbers or private email addresses.

Reporting Incidents

- I will inform a member of the network management staff in writing immediately of any websites accessible from within school I feel are unsuitable in any way for student consumption.
- I understand my part in maintaining the accuracy of the filtering system.
- I will inform a member of the network management staff in writing immediately of abuse of any ICT system(s) – software and hardware – providing the location and names where possible.
- I will inform a member of the network management staff immediately of **ANY** inappropriate content suspected to be on the ICT system(s). This may be contained in email, documents, pictures etc.
- I will report any breaches, or attempted breaches, in security to a member of the network management staff in writing immediately.

Software, Hardware, Copyright and Licensing

- I will not attempt to install any software or hardware.
- **BEFORE** purchasing any hardware or software I will consult a member of the network management staff to check compatibility, license compliance and discuss any other implications that the purchase may have.
- I will respect copyright and make sure I do not use any information breaching copyright law.
- Under **NO** circumstances must any software from potentially illegal sources be installed.
- I will not engage in activities that waste technical support time and resources.

Signature: …… **Date: …….**