E-SAFETY POLICY

THIS POLICY IS REVIEWED ON AN ANNUAL BASIS

Policy reviewed by: John Taylor – Headmaster

Policy approved by: Robert Berry – Director of Operations

Review date: 01/09/2020

Submission: 01/09/2020

Version: v3.0

Policy actioned from: September 2020

Next review date: 31/08/2021

Reviewer's Signature: 

Approver's Signature: 

Please note: 'School' refers to Chatsworth Schools; 'parents' refers to parents, guardians and carers.

This is a whole School policy, which also applies to the Early Years Foundation Stage.

The E-Safety Coordinator is Nin Chohan

The importance of Internet use:

- Internet use is part of the statutory curriculum and is a necessary tool for learning.
- 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.
- 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 access is an entitlement for students who show a responsible and mature approach to its use.

Benefits of Internet Use to Education

Benefits of using the Internet in education include:

- Access to worldwide educational resources including museums and art galleries;
- Educational and cultural exchanges between pupils worldwide;
- 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

The School's Internet Access will be designed to enhance and extend education:

- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- The School will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils comply with copyright law.

- Access levels to the Internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

Teaching Pupils to Evaluate Internet Content

- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will use age-appropriate tools to research Internet content.
- Pupils will be given clear guidance by their teacher on the use of technology in the classroom and beyond.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-School requirement across the curriculum.

Maintenance of Information Security Systems

- The security of the School information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet or taken off site will be encrypted.
- Portable personal media may not be used without specific permission followed by an anti-virus / malware scan.
- Unapproved software will not be allowed in work areas or attached to email. Files held on the School's network will be regularly checked.
- The IT coordinator/network manager will review system capacity regularly.
- The use of user logins and passwords to access the School network will be enforced.
- Staff will receive regular training on online safety.

Management of E-mail

- Pupils will only use the School-provided email for communication with staff.
- The management of personal data will always be in line with statutory requirements.
- Staff will only use official School provided email accounts to communicate with pupils and parents/carers, as approved by the Senior Leadership Team
- Publishing of pupils' images and work

- Images or videos 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.
- Written permission from parents or carers will be obtained before images/videos of pupils are electronically published.
- Pupils' work can only be published with their permission or the parents.
- Written consent will be kept by the School where pupils' images are used for publicity purposes, until the image is no longer in use.
- The School will have a policy regarding the use of photographic images of children, which outlines policies and procedures

Management of the Use of Social Networking, Social Media and Personal Publishing

- The School will control access to social media and social networking sites.
- 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/family, specific interests and clubs, etc.
- Staff wishing to use Social Media tools with students as part of the curriculum will risk-assess the sites before use and check the site's terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the Senior Leadership Team before using Social Media tools in the classroom.
- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- All members of the School community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of School) will be raised with their parents/carers, particularly when concerning students' underage use of sites.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction, and safe and professional behaviour will be outlined in the School's Acceptable Use Policy.

Management of Web-Filtering

- The School's broadband access will include filtering appropriate to the age and maturity of pupils. The School will have a clear procedure for reporting breaches of

filtering. All members of the School community (all staff and all pupils) will be aware of this procedure.

- If staff or pupils discover unsuitable sites, the URL will be reported to the School e-Safety Coordinator who will then record the incident and escalate the concern as appropriate.
- The School's filtering system will block all sites on the Internet Watch Foundation (IWF) list. Changes to the School filtering policy will be risk-assessed by staff with educational and technical experience prior to any changes and, where appropriate, with consent from the Senior Leadership Team.
- The School Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective.
- Any material that the School believes is illegal will be reported to appropriate agencies. The School's access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from network managers.

Management of Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in School is allowed.
- Pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the School Acceptable Use of Mobile Phone Policy.

Protection of Personal Data

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

Authorisation of Internet Access

- The School will maintain a current record of all staff and pupils who are granted access to the School's electronic communications.
- All children are required to sign the IT Code of Conduct.
- All visitors to the School site who require access to the School's network or Internet access will be asked to read and sign an Acceptable Use Policy.
- Parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability.
- When considering access for vulnerable members of the School community (such as with children with special education needs) the School will make decisions based on the specific needs and understanding of the pupil(s).
- At Key Stage 1 pupils' access to the Internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials.

- At Key Stage 2 and 3 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed, where necessary.

Assessment of Risk

- 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. Neither the School nor CS can accept liability for the material accessed, or any consequences resulting from Internet use.
- The School will audit ICT use to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate.

School Response to Incidents of Concern

- All members of the School community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyber bullying, illegal content, etc.).
- The Head will record all reported incidents and actions taken in the School e-Safety incident log and in any other relevant areas, e.g. Bullying or Child Protection log.
- The Designated Safeguarding Lead will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The School will manage e-Safety incidents in accordance with the School discipline/behaviour policy, where appropriate.
- The School will inform parents/carers of any incidents of concerns, as and when required.
- After any investigations are completed, the School will debrief, identify lessons learnt and implement any changes required.

Handling of E-Safety Complaints

- Complaints about Internet misuse will be dealt with under the School's complaints procedure. Any complaint about staff misuse will be referred to the Head.
- All e–Safety complaints and incidents will be recorded by the School, including any actions taken.

Management of Cyber Bullying Issues

- Cyber bullying (along with all other forms of bullying) of any member of the School community will not be tolerated. Full details are set out in the School's policy on anti-bullying and behaviour.
- There are clear procedures in place to support anyone in the School community affected by cyber bullying.

- All incidents of cyber bullying reported to the School will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of cyber bullying.
- The School will take steps to identify the bully, where possible and appropriate. This may include examining School system logs, identifying and interviewing possible witnesses and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the School to support the approach to cyber bullying and the School's e-Safety ethos.

Management of the Use of the Learning Platform

- The SLT and staff will regularly monitor the usage of the Learning Platforms by pupils and staff in all areas, in particular, message and communication tools and publishing facilities.
- Pupils/staff will be advised about acceptable conduct and use when using the LP.
- All use of the LP by staff, pupils and parents will be logged and can be tracked by administrators. 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 on to the LP. When staff, pupils, etc. leave the School their account or rights to specific School areas will be disabled.

Management and Use of Mobile Phones and Personal Devices

- The use of mobile phones and other personal devices by students and staff in School will be decided by the School and covered in the School Acceptable Use or Mobile Phone Policies.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the School community and any breaches will be dealt with as part of the School discipline/behaviour policy.
- School staff may confiscate a phone or device if they believe it is being used to contravene the School's behaviour or bullying policy. The phone or device might be checked by the Senior Leadership team with the consent of the pupil or parent/carer. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.
- Mobile phones will not be used during lessons or formal School time unless as part of an approved and directed curriculum-based activity, with consent from a member of staff.
- Electronic devices of all kinds that are brought into School are the responsibility of the user. The School accepts no responsibility for the loss, theft or damage of such items. Nor will the School accept responsibility for any adverse health effects caused by any such devices either potential or actual.

Introduction of the Policy to Pupils

- All users will be informed that network and Internet use will be monitored.
- An e–Safety training programme will be established across the School to raise the awareness and importance of safe and responsible Internet use amongst pupils. This training will happen regularly.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.

Discussion of the Policy with Staff

- The E–Safety Policy will be formally provided to and discussed with all members of staff. To protect all staff and pupils, the School will implement Acceptable Use Policies.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.

E-Safety Contacts and References

School E-Safety coordinator – Nin Chohan

CEOP (Child Exploitation and Online Protection Centre): Childline: www.childline.org.uk

Childnet: www.childnet.com

Click Clever Click Safe Campaign: http://clickcleverclicksafe.direct.gov.uk

Cybermentors: www.cybermentors.org.uk

Digizen: www.digizen.org.uk

Internet Watch Foundation (IWF): www.iwf.org.uk

Kidsmart: www.kidsmart.org.uk

Teach Today: http://en.teachtoday.eu

Think U Know website: www.thinkuknow.co.uk

Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com

Interpretation

In this policy, the term "senior manager" means a School Head and their designated deputies.

This policy applies to all employees in all Schools (save for Schools with their own procedure which shall prevail) and other work environments within Chatsworth Schools

This policy applies within all companies, which are wholly owned subsidiaries of Chatsworth Schools Ltd, a company registered in England, registered number 11552579.

The registered office of all companies is Crimea Office, The Great Tew Estate, Great Tew, Chipping Norton, Oxfordshire, OX7 4AH. Any enquiries regarding the application of this policy should be addressed to the Director of Operations at the above address.

CHATSWORTH SCHOOLS

PATTISON COLLEGE

POLICY AMENDMENT PAGE

Date	Key Amendments	Version Number	Signed off by
13/03/2020	Approved Policy. – Fit for use	v2.0	RNB