CHATSWORTH SCHOOLS

ONLINE SAFETY POLICY

THIS POLICY IS REVIEWED ON AN ANNUAL BASIS

Policy reviewed by: Andrew Greenway - Director of Information

Review date: 01/06/2024

Submission: 01/06/2024

Version: v7.0

Policy actioned from: 1 September 2024

Next review date: 01/06/2025

Reviewer'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.

CHATSWORTH SCHOOLS

POLICY AMENDMENT PAGE

Date	Key Amendments	Version Number	Reviewed by
16/03/2020	Policy Approved	v2.0	RNB
10/12/2020	Annual Review	v3.0	RNB
01/07/2021	Policy updated	v4.0	AMG
01/07/2022	Annual Review	v5.0	AMG
01/07/2023	Annual Review	v6.0	AMG
01/06/2024	Annual Review	v7.0	AMG

Responsibilities

Online safety depends on staff, schools, governors, advisers, parents and pupils taking responsibility for the safe use of Internet and associated communication technologies. The balance between education for responsible use, regulation and technical solutions must be judged carefully.

It is acknowledged that, whilst the school provides pupils with a protected environment for Internet usage in school, the pupils may not benefit from the same level of protection in their access to the Internet beyond the confines of the school. Important aspects of the school's online safety provision are, therefore, the development of the pupils' understanding of keeping safe online when not at school and supporting parents in understanding how to help keep their children safe online.

The headteacher, DSL and DDSLs are responsible for ensuring, so far is reasonably practicable, a safe environment for internet use, for the implementation of policy and for the development of the pupils' understanding of how to keep themselves safe online, both in and out of school. As required by 'Keeping Children Safe in Education', a member of the DSL team has specific responsibility for the oversight of the quality of online learning and provision in the school.

The ICT Manager is responsible for the maintenance of hardware and software systems and technology to ensure, so far as is reasonably practical, safe use of the Internet.

The Academic ICT co-ordinator is responsible for overseeing the successful development, both in ICT/Computing lessons and the wider curriculum and extra-curricular activities, of pupils' understanding of how to keep safe online and for supporting staff in implementing this objective.

All staff and volunteers are responsible for monitoring pupils' safety online, reporting any concerns arising from pupils' internet use, either at school or at home, and for supporting the development of the pupils' understanding of how to keep themselves safe online. Schools will ensure that, as part of the requirement for staff to undergo regularly updated safeguarding training and the requirement to ensure children are taught about safeguarding, including online safety, that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach.

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 pupils 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 and welfare, to support the professional work of staff and to enhance the school's management functions.
- Internet access is an entitlement for pupils 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 and online training;
- 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 is designed to enhance and extend education:

- Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- The school seeks to ensure that the copying and subsequent use of Internet-derived materials by staff and pupils comply with copyright law.
- Access levels to the Internet are reviewed to reflect the curriculum requirements and the age and ability of pupils.
- Staff are asked to guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.
- Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

- Pupils are 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 are taught to be critically aware of the materials they read and are shown how to validate information before accepting its accuracy.
- Pupils use age-appropriate tools to research Internet content.
- Pupils are 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 viewed as a whole-school requirement across the curriculum.
- Throughout the curriculum and, in particular, in ICT/Computing and PSHE lessons, the school ensures that pupils develop resilience to online threats and an age-appropriate understanding of how to keep safe online, both at and away from school. This includes not sharing personal information and understanding how to recognise and report concerns.

Maintenance of Information Security Systems

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Updates will be applied via a central system to maintain security in a timely fashion.
- 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 is not allowed in work areas or attached to email. Files held on the school's network will be regularly checked.
- The IT coordinator/network manager reviews system capacity regularly.
- The use of user logins and passwords to access the school network will be enforced – IAW the Chatsworth Schools Password Policy.
- Staff receive regular training on online safety, as expected in 'Keeping Children Safe in Education' including the annual Cyber Security Course.

Technical Provision

Antivirus protection and patch management is provided by ICTn and filtering and monitoring is provided by ICTn. FortiGate devices provide 'edge protection' such that any device connected to the school's networks is monitored and inappropriate content is blocked.

Management of E-mail

- In age ranges where pupils are allocated school email addresses, they communicate by email with staff using only their school-provided email, addressing staff only on the member of staff's school email address.
- The management of personal data is always in line with statutory requirements.
- Staff use only official school-provided email accounts to communicate with pupils and parents/carers, as approved by the Senior Leadership Team and in accordance with the Chatsworth Schools E-Mail Policy.

Publishing of pupils' images and work

- Images or videos that include pupils are selected carefully, with the intention of not providing material that could be reused.
- Pupils' full names are not used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers is obtained before images/videos of pupils are electronically published. Such permission may be sought on an on-going basis when the pupil joins the school.
- Pupils' work can be published only with the permission or their parents.
- Written consent is kept by the school where pupils' images are used for publicity purposes, until the image is no longer in use.
- The 'Use of cameras' section of the school's safeguarding policy provides details of the policy regarding the taking and use of photographic images of children.

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

- Through its filtering and monitoring and the restrictions places on the use of personal devices, the school controls access on the school site to social media and social networking sites.
- Pupils are 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 pupils 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 are required to obtain documented consent from the Senior Leadership Team before using Social Media tools in the classroom.
- Pupils learn about security and privacy online and are encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupils are 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 pupils' use of social networking, social media and personal publishing sites (in or out of school) are discussed with the Designated Safeguarding Lead, in accordance with the safeguarding policy and raised with their parents/carers, particularly when concerning pupils' underage use of sites.
- Staff personal use of social networking, social media and personal publishing sites is discussed as part of staff induction and general safeguarding training; safe and professional behaviour is outlined in the staff code of conduct and the Acceptable Use Policy.

Management of Web-Filtering

- The school's broadband access includes filtering appropriate to the age and maturity of the pupils. The school has a clear procedure for reporting breaches and attempted breaches of filtering. All members of the school community (all staff and all pupils) are made aware of this procedure.
- If staff or pupils discover unsuitable sites, the URL will be reported to the School online safety Coordinator who then records the incident and escalate the concern as appropriate. The Designated Safeguarding Lead will be informed if the matter may indicate a safeguarding concern.

- The School's filtering system is configured to block all sites on the Internet Watch Foundation (IWF) list. Changes to the school filtering policy are risk-assessed by staff with educational, safeguarding and technical experience prior to any changes and, where appropriate, with consent from the Senior Leadership Team.
- The School Senior Leadership Team ensures that regular checks are made to ensure that the filtering methods selected are effective. Staff undertaking such checks will usually include the Designated Safeguarding Lead; checks will never be undertaken by one person alone and the headteacher will be alerted in advance of the day and time of the exercise.
- Any material that the school believes is illegal will be reported to appropriate agencies. The school's access strategy will be designed by the school's education and safeguarding specialists to suit the age and curriculum requirements of the pupils, with advice from network managers.

Management of Emerging Technologies

- Emerging technologies are examined for educational benefit and a risk assessment is carried out before use in school is allowed.
- Pupils are instructed about safe and appropriate use of personal devices both on and off site, in accordance with the school Acceptable Use of IT/Mobile Phone Policy/Code of Conduct.

Protection of Personal Data

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

Authorisation of Internet Access

- The school maintains 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 annually.
- All visitors to the school site who require access to the school's network or Internet access are asked to read and sign an Acceptable Use Policy.
- Parents are 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 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed, where necessary.
- At Key Stage 3 and beyond, at an age-appropriate level, pupils may have times, for example during personal study, when they are allowed Internet access through the school's filtering and monitoring, via remote supervision.

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 Chatsworth Schools can accept liability for the material accessed, or any consequences resulting from Internet use. Any such incident will be thoroughly investigated and appropriate action taken.
- The school audits ICT use to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate.

School Response to Incidents of Concern

- All members of the school community are informed about the procedure for reporting online safety concerns (such as breaches of filtering, cyber bullying, illegal content, etc.).
- The Head records all reported incidents and actions taken in the School online 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 online safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The school will manage online safety incidents in accordance with its staff discipline or pupil behaviour policy, where appropriate.
- The school informs 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 Online 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 online safety complaints and incidents are recorded by the school, including any actions taken and the dates of resolution.

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 policies on anti-bullying and behaviour.
- Clear procedures are 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.
- Incidents or allegations of cyber bullying are investigated in accordance with the school's anti-bullying and safeguarding policies.
- 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, Children's Social Care and the police, if necessary.
- Pupils, staff and parents/carers are required to work with the school to support the approach to cyber bullying and the school's online safety ethos.

Management of the Use of the Learning Platform – Where Deployed

- The SLT and staff 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 and staff are advised about acceptable conduct and use when using the Learning Platform.
- All use of the Learning Platform by staff, pupils and parents is logged and can be tracked by administrators. Only members of the current pupil, parent/carers and staff community have access to the Learning Platform. All users need to be mindful of copyright issues and upload only appropriate content on to the Learning Platform. When staff, pupils and any volunteers with access 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 pupils and staff must be in accordance with the school's Safeguarding Policy, its Acceptable Use or Mobile Phone Policies and any additional guidance and procedures provided.
- The sending of abusive or inappropriate messages or content, by any member of the school community, via mobile phones or personal devices, is forbidden. Any breaches will be dealt with as part of the staff discipline and pupil behaviour policies, as relevant.
- School staff may confiscate a phone or device if they believe it is being used to contravene the school's behaviour or bullying policies. The phone or device might be checked by the Senior Leadership team with the consent of the pupil or parent/carer. If there is a serious concern, the Head is authorised to check the content of a mobile phone with or without the permission of the pupil of 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. For further information on searching and confiscation, please refer to the behaviour policy.
- 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 in to 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 are informed that network and Internet use is monitored.
- An online safety training programme has been established across the school to raise the awareness and importance of safe and responsible Internet use amongst pupils. This training is embedded across the curriculum and also through key extra-curricular elements, such as assemblies, circle time and tutor periods.
- Safe and responsible use of the Internet and technology will be reinforced across all subject areas across the curriculum.

Discussion of the Policy with Staff

- The Online Safety Policy is formally provided to and discussed with all members of staff. It forms part of the induction of new staff. To protect all staff and pupils, the school implements Acceptable Use Policies and Agreements for both staff and pupils.
- Staff are made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Acknowledgement of the policy having been read and understood is included on the Annual Affirmation Sheet for Staff.

Working with Parents

The school recognises that the development of the pupils' understanding of online safety and their resilience to online threats, both at school and beyond the school gates, benefits from a strong relationship with parents. The school works closely with parents to develop and maintain their understanding of online safety so that they are well-equipped to support their children in keeping safe. This includes;

- Parents having access to the school's e-safety policy, either online or from the school office.
- Parents being informed that pupils are provided with supervised Internet access.
- Depending on the age of the pupil, parents and/or their child being asked to sign and return an acceptable use agreement.
- The periodic organisation of online-safety information meetings for parents, which may involve an external speaker.
- Through newsletters, the website and other documentation, keeping parents informed about topical online issues, such as unsuitable online games and social media sites which their children may be attracted to.

Online Safety Contacts and References

School online safety coordinator – Charlie Northcote

Designated Safeguarding team member with responsibility for overseeing online safety – Debbie Green

DfE guidance: Teaching Online Safety in School

CEOP (Child Exploitation and Online Protection Centre): Childline: www.ceop.police.uk

Childnet: www.childnet.com

UK Council for Internet Safety

CybermentorsPLUS: www.cybermentorsplus.org

Digizen: www.digizen.org.uk

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

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 the 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 Information at the above address.

This policy does not form part of any employee's contract of employment and may be amended at any time.