Cressex Lodge Online Safety Policy

Author/Contact:	Dan Bunker – Senior Leader
Approval/Ratified by:	Sarah Snape – Head Teacher
Publication Date:	01/12/20
Review Date:	01/07/21

Policy Statement

We recognise that pupils' use of the internet is an important part of their education but that there are risks associated with its use. The DfE's 'teaching online safety in school' guidance (June, 2019) offers guidance on how to minimise those risks in school and teach children how to stay safe when using the internet in their lives outside of school.

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside of school. The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of our wider duty of care to which all who work in schools are bound. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote achievement.

Unfortunately, the use of these new technologies can put pupils at risk within and outside school. Pupils are not allowed to have any mobile device on them during the school day (we are a 'phone-free school'). This helps to safeguard pupils and ensure they are not accessing any inappropriate material, taking photographs or videos, or communicating with each other on their personal devices. We also have a pro-active monitoring regime which allows us to monitor all internet use. While filters should not 'over block', as it may place unreasonable restrictions on what pupils can be taught, it is also fundamental to be aware of some of the potential dangers that the internet can pose, including:

- Access to illegal, harmful or inappropriate images, video games or other content
- Unauthorised access to/loss of/sharing of personal information
- The risk of being subject to grooming
- The sharing/distribution of personal images without an individual's consent or knowledge
- Inappropriate communication/contact with others, including strangers
- Sexting

- Implications of geolocation (being able to track someone's location via a mobile phone or internet-connected computer)
- Cyber-bullying
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- The potential for excessive use which may have a negative impact on the social and emotional development and learning of the young person.

Teaching pupils about the safe use of technology is embedded throughout the curriculum and the therapy programme and pupils are taught about online safety and risks as part of our whole-school approach.

This policy pays regard to the government guidance issued by the UK Council for Internet Safety https://www.gov.uk/government/organisations/uk-council-for-internet-safety and should be read in conjunction with 'keeping children safe in education, 'relationships and sex education' and 'anti-bullying' policies.

Procedure

The Internet

We have a duty to provide pupils with quality internet access as part of their learning experience. Pupils will be taught what internet use is acceptable and what is not and given clear objectives for its use. All staff involved with teaching and learning will prepare pupils to benefit safely from the opportunities presented and ensure that they have a growing understanding of how to manage the risks involved in online activity by:

- Discussing, reminding or raising relevant online safety messages with pupils routinely, wherever suitable opportunities arise
- Reminding pupils, colleagues and parents/carers about their role and responsibilities around internet safety
- Staff will guide pupils to online activities that will support the learning outcomes planned for the pupils' age and maturity. Access levels will also be reviewed to reflect curriculum requirements
- Teaching pupils as a planned element of personal, social, health, economic and citizenship education about online safety, cyber-bulling, misuse of technology, the law in this area and how to correctly use modern technology for positive reasons.

Managing and Safeguarding Computer Systems

The school commission IT consultants whose responsibilities include ensuring the personal safety of staff and pupils in terms of our IT provision. It is also the IT consultants' role to work with the leadership team to ensure that the security of the schools systems and its users are reviewed regularly. To support the maintenance of the schools' IT system:

- Workstations are secured against user mistakes and deliberate actions

- Our servers are located securely and physical access is restricted to appropriate staff
- The server operating system is secured and kept up to date
- A firewall is maintained and virus and malware protection for the whole network is installed and current
- Virus protection is installed and current on all laptops used for school activity
- Access by wireless devices is proactively managed (pupils cannot access the school's wireless network unsupervised)
- Portable media may not be used without specific permission followed by a virus check
- Unapproved software is not allowed on any school machines
- Files held on the schools' network are regularly checked
- IT consultants will review system capacity regularly
- Any administrator or master passwords for school IT systems are kept secure and available to at least two members of staff, e.g. the Chief Executive (CE) and the designated safeguarding lead. The password is changed termly to maintain a high level of security.
- No-one except the IT consultants, the CE or designated safeguarding lead is allowed to download and install software onto the network
- New users can only be given access by the IT consultants, once permission is given by a member of the leadership team
- Any laptops or school technology taken off school sites must be used in accordance with this and all other relevant school policies and any damage or loss is at the expense of the staff member

Monitoring and Filtering Internet Access

Internet usage at Cressex Lodge School is filtered and monitored by a system called Netsweeper. This allows members of the leadership team and governors to check all internet usage, both staff and pupils. Our IT consultant and the DSL receive alert notifications and weekly summaries of activity from Netsweeper and are able to immediately filter information in order to highlight potentially concerning activity and identify the user involved. The advanced filtering and monitoring made available to us by Netsweeper goes above and beyond that which is mandated in 'Keeping Children Safe in Education' (September, 2020) and the DfE 'Teaching online safety in school' guidance (June, 2019).

- Staff are required to be extra vigilant in monitoring pupils when using any internet-capable device
- The wireless network is secure and is password-protected, which prevents unauthorised access. Users will be required to enter their username and password before being able to access the network from any device
- Staff have access to administer/download PCs and laptops that are part of our domain and they have LOCAL ADMIN access only

- A firewall is installed on the schools' networks, which provides web/content filtering, ensuring that reasonable precautions are taken to prevent access to inappropriate material. However, it is not always possible to guarantee that access to unsuitable material will never occur

- Teachers are encouraged to inspect websites they wish to use beforehand and will be responsible for all pupils who access the internet in their lessons
- Additional filtering may be installed by the schools as and when required
- All users are informed about what to do if inappropriate material is accessed or found on the computer

Network Access

There are robust systems in place for managing network accounts and passwords, including safeguarding administrator passwords.

- All users are provided with a log-in appropriate to their role within the schools
- Pupils are taught about safe practice with regard to login and password information
- All passwords are changed regularly to maintain a high level of security
- Access to personal, private or sensitive information and data is restricted to authorised users only, with proper procedures being followed for authorising and protecting login and password information
- Remote access to school systems is limited and covered by specific agreements and is never allowed to unauthorised third-party users

Email

Email is regarded as an essential means of communication and all employees are provided with an e-mail account. Communication by email from teaching staff and administration staff to parents/carers and to external organisations should be related to school matters only. Email messages related to school matters should reflect a suitable tone and content, ensuring that the good name of the schools is maintained.

The same procedures are expected of all other employees who send emails to external organisations and colleagues.

Staff should not use personal email accounts during school hours or for professional purposes. Staff are not permitted to use school email accounts to communicate with pupils at any time.

Publishing Material Online

www.swaay.co.uk

Cressex Lodge School as part of SWAAY Adolescent & Children's Services maintains editorial responsibility for website content to ensure that the content is accurate and the quality of presentation is maintained. The schools maintain the integrity of their website by ensuring that responsibility for uploading material is always moderated and that passwords are protected.
The identities of pupils are protected at all times. Cressex Lodge avoids using photographs of its pupils in order to protect their identity, however, should there ever be reason for their use, photographs of individual pupils are not published on the website unless parents/carers/legal guardians have provided written permission for the school to use pupils' photographs. Photographs never have names attached.

Pupils publishing online (blogs and websites)

In some instances, it may be appropriate for pupils to use websites or blogs to complete, or celebrate, their work. As always, the identities of pupils must be protected at all times. Photographs of identifiable individual pupils are not published unless parents/carers have provided written permission for the school to use pupils' photographs. Photographs must never have full names attached (first name or initials only) and no personal information that could be used to identify them should be disclosed. Parents/carers must have given specific permission via the user agreement forms to allow pupils to create websites or blogs.

Other online communication platforms

Staff and pupils are encouraged to adopt similar safe and responsible behaviour in their personal use of blogs, wikis, social networking sites and other online publishing inside and outside of school hours. Material published by pupils and staff in a social context which is considered to bring the schools' reputation into disrepute or considered harmful to, or harassment of, another child or member of the organisation will be considered a breach of conduct and behaviour and treated accordingly, as per our behaviour, equality, preventing and responding to bullying and/or staff conduct policy/procedures.

Using Images, Video and Sound

Cressex Lodge School recognises that many aspects of the curriculum can be enhanced by the use of multi-media and that there are now a wide and growing range of devices on which this can be accomplished. Pupils are encouraged and taught safe and responsible behaviour when creating, using and storing digital images, video and sound.

Digital images, video and sound recordings are only taken with the permission of participants; images and video are of appropriate activities and are only taken of pupils wearing appropriate dress. Full names of participants are not used either within the resource itself, within the file-name or in accompanying text online.

All parents/carers/legal guardians are asked to sign an agreement about taking and publishing photographs and video of their pupils when offered a school or activity placement and this list is checked whenever an activity is being photographed or filmed.

For their own protection staff or other visitors to our premises are not permitted to take photographs using a personal device (mobile phone, digital camera or digital video recorder) of pupils or visitors.

Mobile Phones

Pupils are discouraged from bringing mobile phones into school but if they do they must hand them to the school offices for safe keeping until the end of the school day. School staff may need to use personal mobile phones during the school day, but this should be done so discretely and out of sight of pupils where possible, unless relating to a school issue (i.e. requiring support in a classroom). Staff should not use personal mobile phones in any situation where their mobile phone number or other personal details may be revealed to a child or parent/carer. Unauthorised or covert use of a mobile phone or other electronic device, to record voice, pictures or video is strictly prohibited.

The sending or forwarding of text messages deliberately targeting a person with the intention of causing them distress, 'cyber-bullying', will be considered a disciplinary matter for pupils and staff alike. The same is the case for other inappropriate use of mobile technology, such as 'sexting'. Pupils are taught about misuse of technology as a matter of course through the therapeutic programme.

New Technology

Cressex Lodge School will keep abreast of new technologies and consider both the benefits for learning and teaching and also the risks from an online safety point of view. We will regularly review this policy to reflect any new technology that we use, or to reflect the use of new technology by pupils.

Employees, visitors or pupils using a technology not specifically mentioned in this policy will be expected to behave with similar standards of behaviour to those outlined in this document.

Data (see our Data Protection & Confidentiality Policy)

The schools recognise their obligation to safeguard staff and pupils' personal data including that which is stored and transmitted electronically. We ensure:

- Pupils are taught about the need to protect their own personal data as part of their online safety awareness and the risks resulting from giving this away to third parties
- Staff are provided with appropriate levels of access to the schools' management information systems (ClearCare) which holds child data.

Passwords are not shared and administrator passwords are restricted and kept securely
- Staff are aware of their obligation to keep sensitive data secure when working on computers outside of school
- When we dispose of old computers and other equipment we take due regard for destroying information which may be held on them
- Remote access to computers is restricted to teachers & leaders
- There is full back up and recovery procedures in place for school data
- Where sensitive staff or child data is shared with other people who have a right to see the information, for example professionals in social care teams, we label the material appropriately to remind them of their duty to keep it secure and securely destroy any spare copies
- All staff sign a contract which includes a confidentiality section when commencing work at SWAAY Adolescent and Child Services.
- Please refer to our data protection policy.

Online Safety Incidents

All incidents, including online safety incidents, are recorded as per other incidents on our online data management system, ClearCare.

Any incidents where pupils do not follow the User Agreement will be dealt with following the school's behaviour policy and procedures.

In situations where a member of staff is made aware of a serious online safety incident, concerning pupils, visitors or staff, they will inform a senior leader who will respond in the most appropriate manner.

Whilst pupils have extremely limited access to social media platforms we are aware that this increases as a pupil goes through the therapeutic group work programme. Instances of cyber-bullying will be taken very seriously and will be dealt with using the schools' preventing and responding bullying procedures and the organisation's disciplinary procedures. The organisation recognises that staff as well as pupils may be victims and will take appropriate action in either situation.

SWAAY Adolescent & Children's Services reserves the right to monitor their premises' equipment and to search any technology equipment, including personal equipment with permission, when a breach of this policy is suspected.

Governance

The Education (Independent School Standards) Regulations apply a duty to proprietors of independent schools to ensure that arrangements are made to safeguard and promote the welfare of children. The body of governance at Cressex Lodge School consists of a proprietorial body and a board of directors.

The proprietorial body and board of directors ensure that they comply with their duties under legislation and fulfil their duty to remedy any weaknesses that are identified. In relation to online safety, duties and responsibilities include:

- The proprietors and board of directors will ensure that appropriate filters and monitoring systems are in place, across all of the sites to ensure that pupils are safeguarded from potentially harmful and inappropriate material
- The proprietors and board of directors will ensure that children are taught about safeguarding, including online, through the therapeutic programme as well as teaching and learning opportunities, as part of providing a broad and balanced curriculum.