Grove Park Academies

ONLINE SAFETY POLICY

Policy For: Grove Park Academies (Grove Park Primary School and Aspire School)

Policy Owner: Ceranne Litton, Executive Headteacher and Chris Denney, ICT Manager

Policy Date: January 2021

Review Date: January 2023

- **The Executive Headteacher will monitor the application of this policy and take appropriate steps to ensure that it is operating effectively.**
- **This policy will be reviewed two-yearly to ensure its effective application.**
- **Linked Policies include:**
  - **General Data Protection (GDPR) Policy**
  - **Complaints and Vexatious Policy**
- **This policy and linked documentation are stored by the central administration team. For further information contact can be made by telephoning: 01795 477417 or emailing admin@groveparkacademies.org**

1 TEACHING AND LEARNING

1.1 Why is internet use important?

- Internet use is part of the statutory curriculum and is a necessary tool for learning.
- The internet is 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, 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 it's use.

1.2 How does internet use benefit education?

- Access to worldwide educational resources including museums and art galleries.
- Access to worldwide educational resources including museums and art galleries;
- Inclusion in the National Education Network which connects all UK schools;
- 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;
- Exchange of curriculum and administration data with KCC and DfE;
- Access to learning wherever and whenever convenient.

1.3 How can the internet enhance learning?

- The school's Internet access is 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 schools will ensure that the copying and subsequent use of Internetderived materials by staff and pupils complies with copyright law.
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- Staff will 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.

1.4 How will pupils learn how to evaluate Internet content?

- Online Safety education will be provided as part of Computing / PHSE /other curriculum areas (as relevant) and will be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school.
- Key online safety messages will be reinforced as part of a planned programme of assemblies and pastoral activities.
- Pupils will be taught in all lessons to be critically aware of the materials /content they access on-line and be guided to validate the accuracy of information.
- Pupils will be helped to understand the need to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet. Rules for use of school computers / laptops / iPads / internet will be devised annually through discussion with pupils. Staff should act as good role models in their use of ICT, the internet and mobile devices.
- 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.
- Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit, thus encouraging responsible use.
- Pupils will be able to practise all they have learnt by contributing to an online blog.

2 STAFF AND PARENT TRAINING

STAFF TRAINING

2.1 Training will be offered as follows:

- Formal online safety training will take place annually for all staff.
- All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy.
- All members of staff (including non teaching) will be made aware of how to recognise and refer any disclosures of incidents involving youth produced sexual imagery. This will be covered within staff training and within the school or college's child protection policy.
- The DSL and ICT coordinator will receive regular updates through training events/LA courses/other information/training sessions and by reviewing guidance documents.
- This online safety policy and its updates will be presented to and discussed by staff in staff meetings
- The DSL (or other nominated person) will provide advice/guidance/training to individuals as required.

PARENT TRAINING

2.2 Training will be offered as follows:

- Parents' attention will be drawn to the schools' online safety policy, newsletters, online safety documents, magazines and the school website and the school will also review whether any online safety workshops are required to support parents' understanding of how best to safeguard their children against potential online dangers.

3 SECURITY; HOW INFORMATION SYSTEMS SECURITY CAN BE MAINTAINED

3.1 Local Area Network (LAN) security issues include:

- Users must act reasonably — e.g. the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use. For staff, flouting electronic use policy is regarded as a reason for dismissal and staff will be dealt with in accordance with the schools disciplinary procedures.
- Workstations should be secured against user mistakes and deliberate actions.
- The server operating system must be secured and kept up to date.
- Virus protection for the whole network must be installed and current.
- Access by wireless devices must be proactively managed and secured with a minimum of WPA2 encryption.

3.2 Wide Area Network (WAN) security issues include:

- Central KPSN Schools Broadband firewalls and local CPEs are configured to prevent unauthorised access between schools.
- Decisions on WAN security are made on a partnership between schools and KCC/EiS.

3.3 The Schools Broadband network is protected by a cluster of high performance firewalls at the Internet connecting nodes in Maidstone and Canterbury. These industry leading appliances are monitored and maintained by a specialist security command centre. The school's web filtering is supplied and managed by EIS Kent and 'Lightspeed' will block any uncategorised websites until they are approved by the ICT manager. This works when using iPads too.

3.4 The security of the school information systems and users will be reviewed regularly.

3.5 Virus protection will be updated regularly.

3.6 Personal data sent over the Internet or taken off site will be encrypted.

3.7 Portable media may not be used without specific permission followed by an anti-virus / malware scan.

3.8 Unapproved software will not be allowed in work areas or attached to email.

3.9 Files held on the school's network will be regularly checked. The ICT coordinator/network manager will review system capacity regularly. The use of user logins and passwords to access the school network will be enforced.

3.10 Personal data protection should be dealt with in the following ways:

- The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused.
- The Data Protection Act 1998 ("the Act") gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information.
- Under the Act every organisation that processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt. The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights let individuals find out what information is held about them. The eight principles are that personal data must be:
    1. Processed fairly and lawfully
    2. Processed for specified purposes
    3. Adequate, relevant and not excessive
    4. Accurate and up-to-date
    5. Held no longer than is necessary
    6. Processed in line with individual's rights
    7. Kept secure
    8. Transferred only to other countries with suitable security measures.
- Schools will already have information about their obligations under the Act, and this section is a reminder that all data from which people can be identified is protected.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

3.11 Emails will be managed in the following ways:

- Staff will only use official school provided email accounts to communicate with pupils and parents / carers, as approved by the Senior Leadership Team.
- Access in school to external personal email accounts may be blocked.
- Excessive social email use can interfere with learning and will be restricted.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
- The forwarding of chain messages is not permitted.

- Staff should not use personal email accounts during school hours or for professional purposes.

3.12 Published content will be managed in the following ways:

- 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 will be published carefully online, to avoid being harvested for spam (e.g. by replacing '@' with 'AT'.)
- The Headteacher will, in consultation with the ICT Manager, take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.
- The school's online blog will be monitored heavily by the class teacher and the ICT coordinator and all posts made publically by the children will be reviewed before posting.

3.13 Publishing pupils work and images:

- 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.

3.14 Social networking, social media and personal publishing will be managed in the following ways:

- 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 email 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 sites 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.
- Staff official blogs or wikis should be password protected and run from the school website with approval from the Senior Leadership Team. Members of staff are advised not to run social network spaces for pupil use on a personal basis.
- Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- 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. Pupil 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.
- Newsgroups will be blocked unless a specific use is approved.
- Concerns regarding pupils' 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 pupils' 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 Acceptable Use Policy. Any staff member who fails to follow school policy may be subject to the schools disciplinary procedures.

4 MANAGING CONTENT AND DEVICES

4.1 Filtering will be managed in the following ways:

- The school's broadband access will include filtering appropriate to the age and maturity of pupils.
- The school will work with KCC and EIS to ensure that filtering policy is continually reviewed.
- 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 DSL who will then record the incident and escalate the concern as appropriate.
- The School 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 such as IWF, Kent Police or CEOP
- 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.

4.2 Emerging technologies are managed in the following ways:

- 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 or Mobile Phone Policy.

4.3 Mobile phones and personal devices will be managed in the following ways:

- The use of mobile phones and other personal devices by pupils and staff in school will be decided by the school and covered as part of the school's induction process.
- 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.
- All incidents involving youth produced sexual imagery or sexting will be referred to the DSL as soon as possible. The DSL will hold an initial review meeting with appropriate school staff and subsequent interviews will take place with the young people involved (if appropriate). Parents will be informed at an early stage and involved in the process unless there is good reason to believe that involving parents would put the young person at risk of harm.
- School staff may confiscate a phone or device if they believe it is being used to contravene the schools behaviour or bullying policy. The phone or device might be searched 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, including youth produced sexual imagery or sexting, the phone will be handed over to the police for further investigation.
- Mobile phones and personal devices will not be used during lessons or formal school time. They should be switched off at all times and Early Years phones need to be kept in the cupboard.
- 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.
- The Bluetooth function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- 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.
- Mobile phones and personal devices are not permitted to be used in certain areas within the school site such as changing areas, toilets.
- If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity then it will only take place when approved by the Senior Leadership Team.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.

5 PUPIL USE OF PERSONAL DEVICES

5.1 Pupils will be required to sign a form to explain their reasoning behind bringing a phone into school. SLT to review these reasons.

5.2 If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school policy.

5.3 Phones and devices must not be taken into examinations. Pupils found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.

5.4 If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

5.5 Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

5.6 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.

5.7 Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.

5.8 If third party materials are to be included, check that recording is acceptable to avoid infringing the third party intellectual property rights.

5.9 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.

6 INTERNET ACCESS

6.1 Internet access will be authorised in the following ways

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- All staff will read and agree to the 'Staff Information Systems Code of Conduct' or School Acceptable Use Policy as presented to them on screen, before using any school ICT resources.
- All visitors to the school site who require access to the schools network or internet access will be asked to read and agree to an Acceptable Use Policy as presented to them on screen, before gaining access to the Internet.
- Parents will be informed that pupils will be provided with supervised Internet access.
- 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.

6.2 Risks will be assessed in the following ways:

- 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 KCC can accept liability for the material accessed, or any consequences resulting from Internet use.
- The school will audit ICT use to establish if the Online Safety policy is adequate and that the implementation of the Online 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 and breaches will be reported to Kent Police.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- All staff will have Prevent training to reduce the risks of radicalisation and will know how to report any signs.

6.3 The School will respond to any incidents of concern in the following ways:

- All members of the school community will be informed about the procedure for reporting online safety concerns (such as breaches of filtering, cyberbullying, illegal content etc).
- The DSL will record all reported incidents in the Bullying or Child protection log.
- The DSL will be informed of any online safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- All staff are aware of the risks posed by online activity of extremists and have a duty to take action is they believe the wellbeing of any pupil is being compromised.
- The school will manage online 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.
- The school will report any signs of radicalisation based on what websites the children have been visiting in relation to the Prevent strategy.
- After any investigations are completed, the school will debrief, indentify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Children's Safeguard Team or online safety officer and escalate the concern to the Police
- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Area Children's Officer or the County online safety Officer.
- If an incident of concern needs to be passed beyond the school then the concern will be escalated to the online safety officer to communicate to other schools in Kent.

6.4 Online safety complaints will be handed as follows:

- Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- Any complaint about staff misuse will be referred to the Headteacher.
- All online safety complaints and incidents will be recorded by the school, including any actions taken.
- Parents and pupils will need to work in partnership with the school to resolve issues.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- Discussions will be held with the local Police Safer Schools Partnership Coordinators and/or Children's Safeguard Team to establish procedures for handling potentially illegal issues.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

6.5 Cyberbullying will be handled as follows:

- Cyberbullying (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 cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded.
- There will be 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.
- 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 cyberbullying and the school's online safety ethos.

6.6 Sanctions for those involved in cyberbullying may include:

- The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
- Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
- Parent/carers of pupils will be informed.
- The Police will be contacted if a criminal offence is suspected.