Granville Sports College

Our Mission Statement

Granville Sports College is committed to:

•Raising standards of achievement and creating opportunities for all pupils, regardless of needs to develop their full potential and improve their life chances.
•Raising the aspirations of the whole school community by creating a culture of continuous learning that celebrates success at all levels.
•Developing a school that is the pride of the local area where pupils, parents, staff, governors and wider community feel valued, listened to and welcomed for the diverse contribution they make to our school life.

Online Safety Policy

E-Safety Co-ordinator:	Mr R Tilley (Deputy Headteacher)
Start date:	Feb 2016
Review date:	Feb 2018 (or in line with new guidance)

Link with other policies:

- ICT Acceptable Use Security Policy
- ICT Agreement – Student and School
- Child Protection and Safeguarding Policy
- Anti-Bullying

Why school need E-Safety Policy

The Governing Board at Granville believes that the use of information and communication technologies in school brings great benefits. Recognising the E-Safety issues and planning accordingly will help to ensure appropriate, effective and safer use of electronic communications.

In today's society, children, young people and adults interact with technologies such as mobile phones, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger.

E-Safety covers issues relating to children and young people as well as adults and their safe use of the Internet, mobile phones and other electronic communications technologies, both in and out of School. It includes

education for all members of the school community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children.

The right balance between controlling access to the internet and technology, setting rules and boundaries and educating students and staff about responsible use. School is aware that children and staff cannot be completely prevented from being exposed to risks both on and offline. Children should be empowered and educated so that they are equipped with the skills to make safe and responsible decisions as well as to feel able to report any concerns. All members of staff need to be aware of the importance of good e-Safety practice in the classroom in order to educate and protect the children in their care. Members of staff also need to understand about how to manage their own professional reputation online and demonstrate appropriate online behaviours compatible with their role.

Breaches of an e-Safety policy can and have led to civil, disciplinary and criminal action being taken against staff, pupils and members of the wider School community. It is crucial that all settings are aware of the offline consequences that online actions can have.

The school have legal obligations to safeguard and protect children on and offline and the accountability of these decisions will sit with the Head Teacher and the Governing Board.

The e-Safety policy is essential in setting out how the School plans to develop and establish its e-Safety approach and to identify core principles which all members of the School community need to be aware of and understand.

Teaching and Learning

- The school Internet access is designed for pupil use and includes filtering appropriate to the age of pupils.
- 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.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access

- Information system security School ICT systems capacity and security will be reviewed regularly.
- Virus protection is robust will be updated regularly.

Management of E-mails account:

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- School reserve the right to monitor emails for the safety of pupils and staff, under the current human rights legislation.

- It is important that staff should use a work provided email account to communicate with parents/carers, pupils and other professionals for any official School business. This is important for confidentiality and security and also to safeguard members of staff from allegations.
- Email accounts should not be provided which can be used to identify both a student's full name and their School. Spam, phishing and virus attachments can make email dangerous.
- 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 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.
- School will have a dedicated email for reporting wellbeing and pastoral issues. This inbox will be managed by designated and trained staff.
- Staff should not use personal email accounts during School hours or for professional purposes.

Published content and the school web site:

Publication of any information online is to be considered from a personal and School security viewpoint. Material such as staff lists, School plan are published in the School handbook and/or on a "staffdocshare" which is secure part of the network which requires authentication.

- The School website comply with the School 's guidelines for publications including publication of the required policies and privacy statements and respect for intellectual property rights and copyright.
- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work:

Small images of groups of pupils should be used and where possible using images that do not show faces at all. Personal photographs can be replaced with self-portraits or images of pupils' work or of a team activity. Pupils in photographs should, of course, be appropriately clothed.

- Written consent will be kept by the School where pupils' images are used for publicity purposes, until the image is no longer in use.
- Pupils' full names will not be used anywhere on the school Learning Platform particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Learning Platform.
- Pupil's work can only be published with the permission of the pupil and parents.
- 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.

Social networking and personal publishing:

- The school 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 or their location.
- Staff wishing to use Social Media tools with students 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 must obtain documented consent from the Head Teacher before using Social Media tools in the classroom.
- Staff official blogs should be password protected and run from the School website with approval from the Head Teacher. Members of staff must not run social network spaces for pupil use on a personal basis.
- All members of the School community are not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- 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 ICT Acceptable use and Security Policy.
-

Managing filtering:

- The school will work with the Local Authority, DCFS and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the named e-Safety person.
- SMT will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Emerging Technologies:

- Mobile phones should not be used during formal school time.
- The sending of abusive or inappropriate text messages is forbidden.
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

How will information systems security be maintained?

The Network Manager in school is aware of security issues of Local Area Network (LAN) 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.
- Workstations will be secured against user mistakes and deliberate actions.
- Server is located securely and physical access restricted.
- The server operating system is secured and kept up to date.
- Virus protection for the whole network must be installed the latest version.
- Access by wireless devices must be proactively managed and secured with a minimum of WPA2 encryption.

Wide Area Network (WAN) security issues include:

- Decisions on WAN security are made on a partnership between School & Derbyshire County Council.

The School Broadband network is protected by a cluster of high performance firewalls. These industry leading appliances are monitored and maintained by a specialist company.

- The security of the School Management Information Systems (MIS) 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 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 and cleared twice a year.
- The ICT Network Manager will review system capacity regularly.
- The use of user logins and passwords to access the School network is enforced.

Protecting personal data:

Personal data will only be recorded, processed, transferred and made available according to the Data Protection Policy.

How will Cyberbullying be managed?

Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone".

There are a number of statutory obligations on School with regard to behaviour which establish clear responsibilities to respond to bullying. In particular section 89 of the

Education and Inspections Act 2006:

- Every School must have measures to encourage good behaviour and prevent all forms of bullying amongst pupils. These measures should be part of the School 's behaviour policy which must be communicated to all pupils, School staff and parents
- Gives Headteachers the ability to ensure that pupils behave when they are not on School premises or under the lawful control of School staff.

Bullying outside School (such as online or via text) is reported to the School, will be investigated and acted on by E-Safety Co-ordinator (RTI).

Although bullying in itself is not a specific criminal offence in the UK, it is important to bear in mind that some types of harassing or threatening behaviour or communications could be a criminal offence, for example under the Protection from Harassment Act 1997, the Malicious Communications Act 1988, the Communications Act 2003, and the Public Order Act 1986. If School staff feels that an offence may have been committed they should seek assistance from the police.

For more information please read "Preventing and Tackling Bullying: Advice for School

Leaders, Staff and Governing Bodies" http://www.education.gov.uk/aboutdfe/advice/f0076899/preventing-andtackling-bullying

DfE and Childnet have produced resources and guidance that can be used to give practical advice and guidance on cyberbullying: http://www.digizen.org/cyberbullying

- Cyberbullying (along with all other forms of bullying) of any member of the School community will not be tolerated.
- 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.

- 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 ICT 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 e-Safety ethos.
- 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 School anti-bullying, behaviour policy or ICT Acceptable Use Policy.
  Parent/carers of pupils will be informed.
  The Police will be contacted if a criminal offence is suspected.

School e-Safety Audit

This self-audit should be completed by the member of the Senior Leadership Team (SLT) responsible for e-safety policy. Staff that could contribute to the audit include: Designated Child Protection Coordinator, SENCO, e-Safety Coordinator, Network Manager and the Head Teacher.

Date of latest update:	
Date of future review:	
The School e-safety policy was agreed by governors on:	
The policy is available for staff to access at:	
The policy is available for parents/carers to access at:	
The responsible member of the Senior Leadership Team is:	
The governor responsible for e-Safety is:	
The Designated Child Protection Coordinator is:	
The e-Safety Coordinator is:	
Were all stakeholders (e.g. pupils, staff and parents/carers) consulted with when updating the School e-Safety Policy?	Y/N
Has up-to-date e-safety training been provided for all members of staff? (not just teaching staff)	Y/N
Do all members of staff sign an ICT Acceptable Use Policy on appointment?	
Are all staff made aware of the School expectation around safe and professional online behaviour?	Y/N
Is there a clear procedure for staff, pupils and parents/carer to follow when responding to or reporting an e-Safety incident of concern?	Y/N

Have e-safety materials from CEOP, Childnet and UE-ACTIS etc. been obtained?	Y/N
Is e-Safety training provided for all pupils (appropriate to age and ability and across all Key Stages and curriculum areas)?	Y/N
Are e-safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils?	Y/N
Do parents/carers or pupils sign an ICT Acceptable Use Policy?	Y/N
Are staff, pupils, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced?	Y/N
Has an ICT security audit been initiated by SLT?	Y/N
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y/N
Is Internet access provided by an approved educational Internet service provider which complies with DfE requirements (e.g. KPSN)?	Y/N
Has the School filtering been designed to reflect educational objectives and been approved by SLT?	Y/N
Are members of staff with responsibility for managing filtering, network access and monitoring systems adequately supervised by a member of SLT?	Y/N
Does the School log and record all e-Safety incidents, including any action taken?	Y/N
Are the Governing Body and SLT monitoring and evaluating the School e-Safety policy and ethos on a regular basis?	Y/N

e-Safety Contacts and References

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

e–Safety Officer, Children's Safeguards Team, Families and Social Care, Derbyshire CC. The e-Safety Officer is: Steve Boyd

Childline: www.childline.org.uk
Childnet: www.childnet.com **Children's Safeguards Team**:
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
LOCAL Police: In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact local Police via 101 or contact your Safer School Partnership Officer. Also visit websites etc.
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

Signed  **Jo Kingswood (Head Teacher)**

Signed  **Karen Mitchell (Chair of Governing Board)**