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.

1. ICT Acceptable Use / Security Policy

Co-ordinator:	Mr D Jackson (Deputy Headteacher)
Start date:	Feb 2016
Review date:	Feb 2018 (or sooner in line with new guidance)

Introduction and Application

Introduction and Application

This policy is applicable to all staff, both teaching and non-teaching. It applies when staff are working in their usual office setting and when staff are working remotely or travelling.

IT is an integral part of all modern business settings and is essential within the context of educational settings. The purpose of the policy is to recognise the need for all staff to be able to utilise school IT systems for the legitimate purposes for which they need it in order to carry out their professional duties.

This policy reflects school broad principles in relation to acceptable use of IT and IT security. It will be subject to further revisions and will be developed so that there will be one suite of documentation relating to e-safety, including individual acceptable use statements signed by staff and by students/parents.

All staff are expected to comply fully with this policy. The Governing Board reserves the right to take disciplinary action in the event that it considers that a member of staff is acting in contravention of this policy. In addition, and in any event the Governing Board reserves the right to consider legal proceedings against any member of staff who breaches this policy.

In the event that a member of staff is any doubt about whether their proposed use of school' IT equipment or systems is in accordance with this policy then they should seek guidance from their manager and or SLT staff before undertaking the activity.

SLT members who are specifically authorised to do so may monitor and inspect any aspect of use of school IT equipment/systems, without prior notice, to the extent permitted by law.

All monitoring, surveillance or investigative activities may be conducted only by Authorised Staff and must comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

1. Password Security

Secure and strong passwords are essential to protect the integrity of IT systems. Strong passwords consist of at least 8 digits and include both letters and numbers.

Staff must always and only use their own passwords when logging into IT systems. Passwords must be changed whenever there is a system prompt to do so or where there is any possibility that there could otherwise be a possible compromise of the system.

Staff should take care to remember their passwords and not to record them anywhere on paper or in an unprotected file. Staff may only use their own passwords. Passwords are always confidential to an individual member of staff and must never be disclosed to another person, including another member of staff.

Where temporary passwords are issued, for any reason (including to new staff) then they should be changed at first logon to a permanent password.

Failure to comply with these requirements can lead to a compromise of the school system security.

2. Acceptable use of email

All staff with professional email accounts have been provided with that email address because it is essential to them being able to carry out their professional duties properly and fully. Professional email accounts are for work related communications and must be conducted via professional email accounts only. The school systems are suitably protected and are the secure and authorised means of conducting work related correspondence. All communications made via professional email accounts must relate to professional duties and be of a tone and nature which reflects the staff member's professional role and the nature of the communication in question.

All online activity, both in school and outside school, must not bring the staff member, in their professional role into disrepute.

Professional email accounts should not be utilised by staff to conduct non work related correspondence.

As detailed above in the Introduction and Application section communications via professional email accounts may be monitored from time to time.

SLT may access a staff member's professional email account if that staff member is absent and there is school related business captured within the account which cannot be otherwise accessed and which requires action before the staff member's anticipated return.

The school recognises that staff will be able to access personal email accounts on school's equipment and that it is reasonable for staff to be able to do so provided that such access:

- Is limited to before and after the staff member's working hours or lunch breaks;
- Is limited to the reading of emails and does not include opening or downloading any attachment received via a personal account without the prior permission. (This requirement is to protect the integrity of school systems).

It is forbidden, at all times, to send files through internal or external email that contain discriminatory, abusive, pornographic, obscene, illegal, offensive, potentially libellous or defamatory content.

3. Acceptable use of internet

Professional Use;

Use of the internet is essential to staff being able to fulfil their professional roles.

The internet may be used to access relevant websites, including for the purposes of teaching and learning in the school. Members of Staff are responsible for undertaking a suitable risk assessment and seeking any necessary authorisations related to of use of the internet in advance of learning taking place.

Personal Use;

The school recognises that staff may need to access the internet for non-work related purposes from School equipment, whilst on School premises or whilst working remotely. As with personal email such access should be limited to before or after the member of staff's working day or during a lunch break and should be for a reasonable period only. Staff may not tie up large proportions of internet resources on non-work related activity, including live internet feeds; down loading video, uploading data / images or audio streams; or making repeated attempts to access a locked website.

In any event staff may not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

Staff personal use of Social Networking sites, personal websites and blogs etc. should make no reference to the School , its pupils, or colleagues (except, in the case of colleagues, with their consent), regardless of whether these sites are accessed while at work or not. Any derogatory comment which expressly or impliedly criticises the School , its staff, pupils or a relevant third party may be cause for disciplinary action (in addition to any claim for defamation).

4. Acceptable use of PCs and network

School PCs are provided to enable staff to fulfil their professional duties.

School PCs may be used to do the following:

- to store School data;
- run software supplied by the School; and
- load text, images, video or audio in connection with normal working requirements.

Staff are responsible for all activity carried out on School systems under any access / account rights assigned to them, whether accessed via School ICT equipment or personal equipment. Therefore staff should not allow any unauthorised person to use School ICT facilities and services that have been provided to them.

Staff may not plug personal ICT hardware into School equipment without specific permission from the relevant member of staff.

Staff must not access, load, store, post or send from School equipment or via a professional email any material that is, or may be considered to be, illegal, offensive, libelous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to School or may bring School into disrepute.

Use of School equipment, systems and networks, should be undertaken in compliance with the Data Protection Act 1998 and the Copyright, Designs and Patents Act 1998. In the event that a member of staff has any concerns as to whether their intended use is duly compatible with relevant legislation then they should seek advice from their manager and/or relevant ICT staff prior to undertaking the activity.

5. Viruses

Viruses can expose School to very considerable risks. All staff are expected to take all reasonable steps to avoid the introduction of any virus on School equipment, systems or networks.

Reasonable steps will include, but are not limited to,

- ensuring that files downloaded from the internet, received via email or on removable media such as a memory stick are checked for any viruses using School provided anti-virus software before being used;

- seeking appropriate permissions before plugging any personal equipment into School equipment.

- not installing any hardware or software without the express permission of the relevant staff member.

- allowing with any anti-virus software installed on School ICT equipment to run as it needs to and not interrupting or in any way interfering with such software;

- ensuring that any IT equipment provided by the School for use off site, benefits from regular School anti-virus updates either by using it to log onto the relevant networks and allowing the updates to run or by providing it to the relevant IT staff so that such updates can be undertaken.

If a member of staff suspects there may be a virus on any School ICT equipment, they must stop using the equipment and contact the ICT Network Manager immediately for further advice.

6. Office telephones

Office/School landline telephones are provided for work related calls.

Phone calls of a personal nature should be kept brief and restricted to matters of importance. Long personal phone calls are not acceptable.

Phone calls to international and premium rate numbers are unacceptable at all times.

7. Remote access – As set out in the Introduction and Application section above remote working and access is covered by this policy in the same way as access on School equipment at school premises.

Staff are, therefore, reminded that all passwords, log ins and access codes remain personal and confidential and must not be disclosed to anyone else. Particular care needs to be taken to avoid any disclosure of such information in a non-work environment and to ensure the staff and responsible retention of all key fobs and other devices necessary for remote access.

Particular care must also always be taking when accessing systems remotely to ensure that screens cannot be viewed other than by the relevant staff member. Staff must ensure their actions are compliant with relevant legislation when accessing systems remotely.

8. Safe use of images

Images of pupils and/ or staff may only be taken, stored and used for professional purposes in accordance with the law and in accordance with school's policies. In any event particular regard must be given to the provision of written consent of the parent, carer or staff member to the taking, storage and use of the images.

Staff are expected to support the School approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the School community.

9. Personal and confidential data

All use of personal and confidential data must be in accordance with the Data protection Act 1998. This applies equally, whether in School premises, taken off the school premises or accessed remotely.

Staff will ensure that personal data is kept secure and is used appropriately. In order to protect personal, sensitive, confidential or classified data and prevent unauthorised access to it, this will include, but may not be limited to;

- Ensuring screen displays of such data are, at all times, be kept out of direct view of any staff who do need to access that information as part of their professional role and out of direct view of any third parties;
- Ensuring screens are locked before moving away from the computer, at any time;
- Ensuring log off from the PC's is fully completed when going to be away from the computer for a longer period of time.
- Ensuring that any print copies made of such data are necessary and that particular care is taken to ensure that printed materials are retained securely and used appropriately.

In the event that a staff member considers that they need to take personal data out of School premises or access it remotely then appropriate authorisation should be sought in advance. Personal or sensitive data taken off site must be encrypted and particular care must be taken when travelling by public transport both to ensure personal data is not inadvertently viewed and to ensure that it is not left behind.

10. School ICT equipment at home

Staff may be supplied with School equipment to utilise at home and outside of their usual work place setting. This includes lap-tops.

Such equipment must be treated and used in the same was as it would be in the workplace. This policy applies in the same way to such equipment as if it were in the work place and staff are expected to abide by this policy when using all such School equipment. This means that staff remain liable for their use of the equipment and their passwords for it.

On request, staff must make portable and mobile ICT equipment available for anti-virus updates and software installations, patches or upgrades. The installation of any applications or software packages must be authorised by the school , fully licensed and only carried out by School ICT Network Manager.

Data must be saved to the School network; Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick or other portable device. If it is absolutely necessary to do so then this should be for as shorter period as possible and the local drive must be encrypted.

Staff are responsible for ensuring that all equipment is stored and kept safely and securely. Any protective equipment must be utilised properly.

On termination of employment, resignation or transfer, staff must return all ICT equipment to the Business Manager and/or ICT Network Manager. Staff must also provide details of all their system logons so that they can be disabled.

The school will dispose of all redundant ICT equipment in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA).

Staff should not be using personal equipment for work purposes. Without prejudice to the school's position, in the event that personal equipment is used for work purposes, when disposing of any such personal device, staff are expected to allow School IT staff to ensure the hard drive is clear of any work files.

Personal and Confidential Data on ICT equipment must never be left unattended in an area accessed by the public and/or when travelling. When travelling by car, if a staff member has to leave the car unattended then ICT equipment should be kept locked in the boot and out of sight.

11. Incident reporting

Staff should report any actual security breaches or attempted security breach, loss of equipment or data, concerns regarding virus, unsolicited emails, any unauthorised use or suspected misuse of ICT or any of matter of concern, to the Business Manager and to relevant ICT staff, as a matter of urgency.

In the event that any member of staff receives an email, through their professional email account, either from within school, DCC or from any third party, which they consider being abusive then that should immediately be reported to the relevant member of staff.

Signed **Jo Kingswood (Head Teacher)**

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