GLENWOOD SECONDARY SCHOOL
EMSWORTH

POLICY ON STAFF ACCEPTABLE USE OF ICT

Reviewed	May 2017
Responsibility to Review	Mark Pratley
Next review	May 2019
Approved	FGB

This policy should be read in conjunction with other policies including Online Safety Policy, Use of Social Media Policy Data Protection and Freedom of Information policies. This Policy was developed using guidance from Hampshire County Council's Manual of Personnel Practice.

Introduction

This policy applies to all employees and volunteers including Governors within the school and in respect of all ICT resources and equipment within the school and resources that have been made available to staff for working at home. ICT resources and equipment includes computer resources, use of school internet access and email systems, software (including use of software such as SAP and SIMS), school telephones and text systems, cameras and recording equipment, intranet and virtual learning environment and any other electronic or communication equipment used in the course of the employee or volunteer's work.

This policy also provides advice to members of staff and volunteers in respect of the potential risks and consequences in relation to inappropriate use of their own personal ICT facilities, where this use is inconsistent with the expectations of staff working with children and young people.

Access

School staff will be provided with a log on where they are entitled to use the school ICT facilities and advised what hardware and software they are permitted to access, including access to the internet and email. Unless indicated, staff can use any facilities available subject to the facilities not being in use by pupils or other colleagues. Access is provided to enable staff to both perform their role and to enable the wider staff in the school to benefit from such facilities.

Where staff have been provided with a school email address to enable them to perform their role effectively, it would not normally be used to communicate with parents and pupils unless express permission has been provided. Where staff are able to access email outside of school hours, the email facility should not routinely be used to undertake school business outside of normal office hours.

Access to certain software packages and systems (e.g HCC intranet; SAP (HR, finance and procurement system), SIMS, RAISE Online, FFT, school texting services) will be restricted to nominated staff and unless permission and access has been provided, staff must not access these systems.

Some staff may be provided with laptops and other equipment for the performance of their role. Where provided, staff must ensure that their school laptop/other equipment is not accessible by others when in use at home and that it is not used inappropriately by themselves or others. Staff must also ensure that they bring their laptop/equipment in as required for updating of software, licences and virus protection.

Where the school provides digital cameras and other recording equipment for educational and school business use and it is used away from the school site, it must be kept secure and safe. Where pictures of pupils are taken, staff must ensure that they ensure consent has been provided by parents, and that the school's policy in relation to use of pictures, is followed.

If the school does not provide school mobile phones, staff may use, in urgent or emergency situations during off site visits, their personal mobile telephones. Where used in these emergency situations and a cost incurred, the school will provide reimbursement of the cost of any calls made. Should staff need to make contact whilst off site, this should normally be undertaken via the school rather than a direct call from the individual's personal mobile. School staff who have access to colleagues' personal contact details must ensure that they are kept confidential.

No mobile telephones or similar devices , even those with hands free facilities should be used whilst driving on school business.

Whether school staff have access to the school telephone system for personal use will be confirmed by the school. Where such use is made of this facility, it must be done during break periods, must not be excessive and the school should require either the cost of the call or a donation to be made towards the cost of the call.

The school will ensure that Display Screen Equipment assessment are undertaken in accordance with its Health and Safety Policy.

Communication with parents, pupils and governors

The school communicates with parents and governors through a variety of mechanisms. The points below highlight who is normally authorised to use which systems and can directly communicate without requiring any approval before use or to agree content. School must indicate to staff if any other staff are permitted to make contact using the systems below:

- School Telephones – all teachers, administrative staff and staff who have been permitted through their roles in pupil welfare or a home/school link staff. Normally teaching assistants and lunchtime supervisory staff would need to seek approval from a member of the senior leadership team where they feel they need to make a telephone call to a parent.
- Text System – All Teachers and Office staff. Where other staff need to send a text, this is normally approved by a member of the Senior Leadership Team.
- Letters – Normally all teachers may send letters home, but they are be required to have these approved by the Headteacher before sending. Where office staff send letters home these will require approval by the School Senior Administrative Officer.
- Email – school email accounts should not be used for communication with parents unless approved by a member of the senior leadership team. Email is used as a normal method of communication amongst school governors and where governors are linked in particular areas with members of staff, communication may take place via email.
- Visits home – All home visits are normally subject to approval by the senior leadership team and must follow the school's policy on home visits.

Under normal circumstances, school staff should not be using any of the methods outlined above to communicate directly with pupils. If a member of staff needs to contact a pupil direct via any of these methods, this must be approved by the Headteacher.

Where pupils are submitting work electronically to school staff, this must be undertaken using school systems and not via personal email.

Social Networking: *Please also read the Use of Social Media Policy*

School staff are advised to exercise extreme care in their personal use of social networking sites, giving consideration to their professional role working with children.

Staff should make appropriate use of the security settings available through social networking sites and ensure that they keep them updated as the sites change their settings. Staff are advised that inappropriate communications that come to the attention of the school can lead to disciplinary action, including dismissal.

Under no circumstances should any school staff have any pupils or any ex-pupils under the age of 18 as friends on their social networking sites. School staff are strongly advised not to have any online friendships with any young people (i.e. including those at other schools) under the age of 18, unless they are family members.

Where school staff do accept friendships via their social networking with ex-pupils aged over 18, they are advised to notify the headteacher. Staff in secondary schools are strongly advised to exercise care and consideration before accepting online friendships with ex-pupils aged under 21. This is particularly relevant where the pupils have left the school recently (e.g. they were a pupil in the school's sixth form) or the pupil or their family have an ongoing relationship with the school (e.g. they have siblings that continue to attend the school).

Schools are encouraged to consider establishing alumni sites enabling former pupils to maintain contact with the school, or provide a mechanism through the school website for former pupils to contact

School staff are strongly advised not to accept friendships via their social networking with parents, ex-parents and governors. Where staff do accept such friendships, they must not engage in any discussion regarding the school whether expressing personal views or opinions or simply recounting events or stating facts.

School staff are able to accept friendships with colleagues via their social networking site but should take care in communications exchanged. Senior staff and those who have line management responsibility are advised to consider the appropriateness of accepting colleagues, particularly those who they manage, as friends on social networking sites. Where accepted, staff should take care to exercise discretion in relation to the communications exchanged.

Where the school uses social networking sites as a means of communication with the school community, school staff must follow the guidance provided by the school in the use of the sites.

Where school staff become aware that there is information about them held on social networking sites that causes them personal concern, they should alert the headteacher to their concern.

Unacceptable Use

Appendix 1 provides a list of Do's and Don'ts for school staff to enable them to protect themselves from inappropriate use of ICT resources and equipment. School systems and resources must not be used under any circumstances for the following purposes:

- to communicate any information that is confidential to the school or to communicate/share confidential information which the member of staff does not have authority to share
- to present any personal views and opinions as the views of the school, or to make any comments that are libellous, slanderous, false or misrepresent others
- to access, view, download, post, email or otherwise transmit pornography, sexually suggestive or any other type of offensive, obscene or discriminatory material
- to communicate anything via ICT resources and systems or post that may be regarded as defamatory, derogatory, discriminatory, harassing, bullying or offensive, either internally or externally

- to communicate anything via ICT resources and systems or post that may be regarded as critical of the school, the leadership of the school, the school's staff or its pupils
- to upload, download, post, email or otherwise transmit or store material that contains software viruses or any other computer code, files or programmes designed to interrupt, damage, destroy or limit the functionality of any computer software or hardware or telecommunications equipment
- to collect or store personal information about others without direct reference to The Data Protection Act
- to use the school's facilities to undertake any trading, gambling, other action for personal financial gain, or political purposes, unless as part of an authorised curriculum project
- to visit or use any online messaging service, social networking site, chat site, web based email or discussion forum not supplied or authorised by the school
- to undertake any activity (whether communicating, accessing, viewing, sharing. uploading or downloading) which has negative implications for the safeguarding of children and young people

Any of the above activities are likely to be regarded as gross misconduct, which may, after proper investigation, lead to dismissal. If employees are unsure about the use of ICT resources including email and the intranet, advice should be sought from a member of the Senior Leadership Team or ICT lead if applicable.

Where an individual accidently accesses a website or material that they consider to be pornographic or offensive, this should be reported immediately to the Headteacher or other member of the senior leadership team. Schools are encouraged to use appropriate blocking software to avoid the potential for this to happen. Reporting to the Headteacher or senior leadership team equally applies where school staff are using school equipment or facilities at home and accidentally access inappropriate sites or material.

Where an individual has been communicated with in a manner outlined above (e.g. has received an inappropriate email or attachment), they are advised to report this immediately to the Headteacher or another member of the senior leadership team so that this can be dealt with appropriately.

Personal and private use

All school staff with access to computer equipment, including email and internet, are permitted to use them for occasional personal use provided that this is access is not:

- taking place at the expense of contracted working hours (i.e. is not taking place during paid working time)
- interfering with the individual's work
- relating to a personal business interest
- involving the use of news groups, chat lines or similar social networking services
- at a cost to the school
- detrimental to the education or welfare of pupils at the school

Excessive personal use of school facilities is likely to be considered to be a disciplinary matter, may lead to restricted access to computer equipment and where costs are incurred (e.g. personal telephone use), the school will seek reimbursement from the member of staff.

It is important for staff to also be aware that inappropriate use of their own personal or other ICT facilities in their personal time, can have implications for their employment situation where this becomes known and the activities that are

undertaken are inconsistent with the expectations of staff working with children and young people.

Where school staff have brought their own personal equipment such as mobile telephones, digital assistants, laptops and cameras, into the school, these personal items, should not be used during pupil contact sessions unless authorised. Staff should follow all points outlined in this section in relation to their personal use. Staff should ensure that there is no inappropriate content on any of these pieces of equipment and ensure that they are not accessed by pupils at any time. Such equipment should not normally be required to enable staff to undertake their role but where it is used, staff should take care to ensure any school data/images are deleted following use of the equipment.

Whilst individuals may be required to use their personal mobile telephone to make contact with the school, staff should exercise care and seek reimbursement.

Security and confidentiality

Any concerns about the security of the ICT system should be raised with a member of the senior leadership team.

Staff are required to ensure that they keep any passwords confidential, do not select a password that is easily guessed and regularly change such passwords.

School staff must take account of any advice issued regarding what is permitted in terms of downloading educational and professional material to the school server. Where staff are provided with a memory pen for such activity, to both protect the integrity of the server and to save space, this should be used. All staff must review the appropriateness of the material that they are downloading prior to downloading and are encouraged to do so from known and reputable sites to protect the integrity of the school's systems. Where problems are encountered in downloading material, this should be reported to the school's ICT lead.

Where staff are permitted to work on material at home and bring it in to upload to the school server through their memory pens, they must ensure that they have undertaken appropriate virus checking on their systems. Where provided, staff should normally use their school issued laptop for such work.

Staff must ensure that they follow appropriate and agreed approval processes before uploading material for use by pupils to the pupil ICT system and/or VLE.

Whilst any members of school staff may be involved in drafting material for the school website, staff must ensure that they follow appropriate and agreed approval processes before uploading material to the website.

The school will nominate staff who are responsible for ensuring that all equipment is regularly updated with new software including virus packages and that licences are maintained on all school based and school issued equipment. Staff must ensure that they notify the nominated staff when reporting any concerns regarding potential viruses, inappropriate software or licences.

Staff must ensure that their use of the school's ICT facilities does not compromise rights of any individuals under the Data Protection Act. This is particularly important when using data off site and electronic data must only be taken off site in a secure manner, either through password protection on memory pens or through encrypted memory pens. This is also particularly important when communicating personal data via email rather than through secure systems. In these circumstances, staff must ensure that they have the correct email address and have verified the identity of the person that they are communicating the data with.

Staff must also ensure that they do not compromise any rights of individuals and companies under the laws of Copyright through their use of ICT facilities.

Monitoring

The Glenwood School uses Hampshire County Council's ICT services and therefore is required to comply with their email, internet and intranet policies.

The school and county council reserve the right to monitor the use of email, internet and intranet communications and where necessary data may be accessed or intercepted in the following circumstances:

- to ensure that the security of the school and county council's hardware, software, networks and systems are not compromised
- to prevent or detect crime or unauthorised use of the school or county council's hardware, software, networks or systems
- to gain access to communications where necessary where a user is absent from work

Where staff have access to the internet during the course of their work, it is important for them to be aware that the school or county council may track the history of the internet sites that have been visited.

To protect the right to privacy, any interception of personal and private communications will not take place unless grounds exist to show evidence of crime, or other unlawful or unauthorised use. Such interception and access will only take place following approval by the Chair of Governors, after discussions with relevant staff in Hampshire County Council's HR, IT and Audit Services and following an assessment to determine whether access or interception is justified.

Whistleblowing and cyberbullying

Staff who have concerns about any abuse or inappropriate use of ICT resources, virtual learning environments, camera/recording equipment, telephony, social networking sites, email or internet facilities or inappropriate communications, whether by pupils or colleagues, should alert the Headteacher to such abuse. Where a concern relates to the Headteacher, this should be disclosed to the Chair of Governors. If any matter concerns child safety, it should also be reported to the Designated Safeguarding Lead.

It is recognised that increased use of ICT has led to cyberbullying and/or concerns regarding e-safety of school staff. Staff are strongly advised to notify their Headteacher where they are subject to such circumstances. Advice can also be sought from professional associations and trade unions. Support is also available through Hampshire's confidential counselling service, Employee Support Line (02380 626606) and also via the UK Safer Internet Centre helpline@safetinternet.otg.uk or 0844 381 4772

Signature

It will be normal practice for staff to read and sign a declaration as outlined in Appendix 2, to confirm that they have had access to the acceptable use policy and that they accept and will follow its terms.

Staff must comply with the terms of this policy. Any breach will be considered to be a breach of disciplinary rules, which may lead to a disciplinary sanction (e.g. warning), dismissal, and/or withdrawal of access to ICT facilities. Staff should be aware, that in certain instances, inappropriate use of ICT may become a matter for police or social care investigations.

PLEASE NOTE: Reference to Staff includes Governors.

Appendix 1

Do's and Don'ts: Advice for Staff

Please also read Social Use of Media Policy

Whilst the wide range of ICT systems and resources available to staff, both in school and outside of school, have irrefutable advantages, there are also potential risks that staff must be aware of. Ultimately if staff use ICT resources inappropriately, this may become a matter for a police or social care investigation and/or a disciplinary issue which could lead to their dismissal. Staff should also be aware that this extends to inappropriate use of ICT outside of school.

This Dos and Don'ts list has been written as a guidance document. Whilst it is not fully comprehensive of every circumstance that may arise, it indicates the types of behaviours and actions that staff should not display or undertake as well as those that they should in order to protect themselves from risk.

General Issues

Do

- ensure that you do not breach any restrictions that there may be on your use of school resources, systems or resources
- ensure that where a password is required for access to a system, that it is not inappropriately disclosed
- respect copyright and intellectual property rights
- ensure that you have approval for any personal use of the school's ICT resources and facilities
- be aware that the school's systems will be monitored and recorded to ensure policy compliance
- ensure you comply with the requirements of the Data Protection Act when using personal data
- seek approval before taking personal data off of the school site
- ensure personal data is stored safely and securely whether kept on site, taken off site or accessed remotely
- report any suspected misuse or concerns that you have regarding the school's systems, resources and equipment to the Headteacher or designated manager and/or Child Protection Liaison Officer as appropriate
- be aware that a breach of your school's Acceptable Use Policy will be a disciplinary matter and in some cases, may lead to dismissal
- ensure that any equipment provided for use at home is not accessed by anyone not approved to use it
- ensure that you have received adequate training in ICT
- ensure that your use of ICT bears due regard to your personal health and safety and that of others

Don't

- access or use any systems, resources or equipment without being sure that you have permission to do so
- access or use any systems or resources or equipment for any purpose that you don't have permission to use the system, resources or equipment for
- compromise any confidentiality requirements in relation to material and resources accessed through ICT systems
- use systems, resources or equipment for personal use without having approval to do so
- use other people's log on and password details to access school systems and resources
- download, upload or install any hardware or software without approval
- use unsecure removable storage devices to store personal data
- use school systems for personal financial gain, gambling, political activity or advertising
- communicate with parents and pupils outside normal working hours unless absolutely necessary

Use of email, the internet and school and HCC intranets

Do

- alert your Headteacher or designated manager if you receive inappropriate content via email
- be aware that the school's email system will be monitored and recorded to ensure policy compliance
- ensure that your email communications are compatible with your professional role
- give full consideration as to whether it is appropriate to communicate with pupils or parents via email, or whether another communication mechanism (which may be more secure and where messages are less open to misinterpretation) is more appropriate
- be aware that the school may intercept emails where it believes that there is inappropriate use
- seek support to block spam
- alert your Headteacher or designated manager if you accidentally access a website with inappropriate content
- be aware that a website log is recorded by the school and will be monitored to ensure policy compliance
- answer email messages from pupils and parents within your directed time
- mark personal emails by typing 'Personal/Private' within the subject header line

Don't

- send via email or download from email, any inappropriate content
- send messages that could be misinterpreted or misunderstood
- use personal email addresses to communicate with pupils or parents
- send messages in the heat of the moment
- send messages that may be construed as defamatory, discriminatory, derogatory, offensive or rude
- use email systems to communicate with parents or pupils unless approved to do so
- download attachments from emails without being sure of the security and content of the attachment
- forward email messages without the sender's consent unless the matter relates to a safeguarding concern or other serious matter which must be brought to a senior manager's attention
- access or download inappropriate content (material which is illegal, obscene, libellous, offensive or threatening) from the internet or upload such content to the school or HCC intranet
- upload any material onto the school website that doesn't meet style requirements and without approval

Use of telephones, mobile telephones and instant messaging

Do

- ensure that your communications are compatible with your professional role
- ensure that you comply with your school's policy on use of personal mobile telephones
- ensure that you reimburse your school for personal telephone calls as required
- use school mobile telephones when on educational visits

Don't

- send messages that could be misinterpreted or misunderstood
- excessively use the school's telephone system for personal calls
- use personal or school mobile telephones when driving
- use the camera function on personal or school mobile telephones to take images of colleagues, pupils or of the school

Use of cameras and recording equipment

Do

- ensure that material recorded is for educational purposes only
- ensure that where recording equipment is to be used, approval has been given to do so
- ensure that material recorded is stored appropriately and destroyed in accordance with the school's policy
- ensure that parental consent has been given before you take pictures of school pupils

Don't

- bring personal recording equipment into school without the prior approval of the Headteacher
- inappropriately access, view, share or use material recorded other than for the purposes for which it has been recorded
- put material onto the school website, school intranet or intranet without prior agreement from a member of the School Leadership Team

Use of social networking sites

Do

- ensure that you understand how any site you use operates and therefore the risks associated with using the site
- familiarise yourself with the processes for reporting misuse of the site
- consider carefully who you accept as friends on a social networking site
- report to your Headteacher any incidents where a pupil has sought to become your friend through a social networking site
- take care when publishing information about yourself and images of yourself on line – assume that anything you release will end up in the public domain
- ask yourself about whether you would feel comfortable about a current or prospective employer, colleague, pupil or parent viewing the content of your page
- follow school procedures for contacting parents and/or pupils
- only contact pupils and/or parents via school based computer systems
- through your teaching, alert pupils to the risk of potential misuse of social networking sites (where employed in a teaching role)

Don't

- spend excessive time utilising social networking sites while at work
- accept friendship requests from pupils or parents – you may be giving them access to personal information, and allowing them to contact you inappropriately
- put information or images on line or share them with colleagues, pupils, or parents (either on or off site) when the nature of the material may be controversial
- post anything that may be interpreted as slanderous towards colleagues, pupils or parents
- use social networking sites to contact parents and/or pupils

Appendix 2:

GLENWOOD SCHOOL: Acceptable Use Agreement (Staff) (2016-17)

Linked to '360° Safe' Guidelines

These guidelines set out the basic principles for how staff use ICT, including the Internet, at Glenwood School and also their use of social networking sites out of school. These principles can be summarised as: ensuring pupils remain safe, ensuring staff remain safe and ensure staff always 'model' good practise. If staff have any questions regarding these guidelines, they should direct them to Senior Leadership Team or the ICT Coordinator. By signing this you agree to the school having the right to examine any content – emails, files, photos etc. and track your internet use.

Report any issues or concerns to the Senior Leadership Team or ICT Coordinator as soon as possible

Use of ICT resources

- Use computers and equipment with care and ensure pupils do the same
- Return cameras and microphones etc. after use (remove pictures/files as data may be deleted)
- Store all photographs in the Photo Gallery drive
  NB: Photos in your personal account or the Curriculum drive will be deleted
- Use resources economically; purchase rechargeable batteries, print in draft and print on both sides of paper
- Scan all removable storage– memory sticks etc. for viruses prior to use
- Do not install software not authorised by the ICT co-ordinator / ICT technician
- Understand that inappropriate use of the school's network may result in some services being removed and further action being taken by the Headteacher
- Return any hardware or equipment if you are no longer employed by the school

Online Behaviour / Safe Working Practises

- Do not share your password with pupils or other staff. If you forget your password it can be easily reset.
- Use a strong password (upper and lower case letters and symbols e.g. $, £ etc.) and change it when required
- **DO NOT** permit pupils to use your account.
- Log off when you have finished using a computer or leave the computer unattended
- Online activity is related to professional duty (although personal use is permitted within reason and does not occur within 'directed time' i.e. lessons etc.
- Do not use the school's ICT resources for financial gain e.g. auction or betting sites or to access inappropriate sites e.g. racist or pornographic sites etc.
- Online dialogue e.g. emails with schools, parents or organisations etc. must remain professional at all times.

Data Protection

- Where data of a personal nature such as school reports, IEPs, photographs, assessment data etc. is taken home on a school laptop or other storage device, it must be recognised that this data comes under the Data Protection Act and is subject to the school's Data Protection Policy. Care must be taken to ensure its integrity and security. It must not be transferred to home computers and should be removed from any portable device including USB pens and memory cards as soon as is practical.
- Where staff are using their own digital equipment e.g. cameras and mobile phones, extreme caution is advised to avoid misinterpretation by others. Files should be transferred to school equipment as soon as possible;

Social Networking

- You must **NOT** correspond with pupils using your own personal social messaging site
- You must **NOT** use any image related to school on any social networking site

- You must **NOT** discuss school related matters on any social networking site
- Pupils attempting to make you a 'friend' or **any** concerns you have **must** be reported to the Headteacher

Please also read:

- **USE OF SOCIAL MEDIA POLICY**
- **GUIDANCE FOR SAFER WORKING PRACTICE FOR ADULTS WHO WORK WITH CHILDREN AND YOUNG PEOPLE** (Sept 2009 and is available in the Child Protection folder held in the staff room). You will be required to complete a new form at the start of each academic year.

Signed _____ Print name _____

Date _____