Calthorpe Park School | Hitches Lane | Fleet | Hampshire | GU51 5JA
t: 01252 613483
e: headteacher.pa@cps.hants.sch.uk
w: www.cps.hants.sch.uk

Head Teacher: Mr Kevan John
Chair of Governors: Mr Jonathan Phillips
Document: Rev 05
Document Next Review Date: May-2026

_____ learners who aspire for themselves and inspire others

E-Safety & ICT Use Policy

(CPS-NS-P-POL-015)

Revision Number	Comments	Date
01	Previous version 2016 – revised by DHT to reflect the new approach to the use of technology. This has been reviewed by a Governor and approved by the FGB.	Nov-21
02	Minor updates following changes in the mobile phone policy, corrected minor grammatical and spelling corrections, and	Dec-22
03	Aligned document to the MOPP Acceptable Use Policy template	Dec-22
04	Revision made after review	May 24
05	Revision made after review	May 25

Endorsement

This policy was endorsed for use by governors electronically on 23 June 2025

Background: Calthorpe Park School is dedicated to providing the best possible education and support for its students. This means having a clear, fair and efficient approach to the use of technology that helps to keep students safe.

Table of Contents

Introduction

Today, 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 occasionally can place young people and adults in danger. Our students should be educated and coached to become safe and respectful 'digital citizens'.
This e-Safety Policy covers issues relating to staff and students and their safe use of the internet, mobile phones and other electronic communications technologies, both in and out of school. It applies to all members of the school community and refers to managing risks, rights and responsibilities. This forms part of our 'duty of care', addresses aspects of the "Keeping Children Safe" agenda, and supports the national Protect campaign.

We must accept that there is a chance that children may be 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 must be aware of the importance of good e-Safety practice in the classroom to educate and protect the children in their care. Members of staff are bound by legislative obligations to ensure they uphold national Teacher Standards by demonstrating appropriate online behaviours.

We share with parents the responsibility to educate our students on e-Safety issues. We must teach students the appropriate behaviours and critical thinking skills which will enable them to remain both safe and compliant with legislation when using the internet and related technologies, in and beyond the context of the classroom.

ICT covers a wide range of resources including desk-top computers, laptops and a variety of mobile devices. Currently the internet technologies staff and students use, both inside and outside of the classroom, include but are not limited to:

- Website and e-learning resources
- Cloud-based applications
- Email and instant messaging
- Social networks
- Blogs, wikis and podcasting
- Desktop and laptops

1. Application

1.1. This policy applies to the school governing body, all teaching and other staff, whether employed by the County Council or employed directly by the school, external contractors providing services on behalf of the school or the County

Council, teacher trainees and other trainees, volunteers and other individuals who work for or provide services on behalf of the school. These individuals are collectively referred to in this policy as staff or staff members.

1.2. The policy applies 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 during the employee or volunteer's work.

1.3. This policy also provides advice to staff 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.

2. Access

2.1. 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.

2.2. 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 can access email outside of school's hours, the email facility should not routinely be used to undertake school business outside of normal office hours.

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

2.4. 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.

2.5. 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.

2.6. 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.

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

2.8. 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.

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

3. Communication with parents, pupils and governors

3.1. 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:

3.1.1. 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.

3.1.2. 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.

3.1.3. Letters – Normally all teachers may send letters home, but they may be required to have these approved by the Year Leader/Head of Department before sending. Where office staff send letters home these will normally require approval by the School Business Manager/Administrative Officer.

3.1.4. 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. When communicating with parents by email, this should be undertaken using the Communicator function in EdulinkOne in order to avoid risk of emails being sent erroneously and removing the need for authentication. Emails sent to individuals should be recorded in the SIMS Communication Log by ticking the relevant box within the Communicator function. It is not necessary to record multi recipient communications in this way.

3.1.5. 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.

3.1.6. Direct communications with students must be undertaken with reserve and only regarding official school matters. Communicate with students using EdulinkOne and ensure that you write any copies of correspondence to the SIMS Communication Log.

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

4. Social Media

4.1. School staff are advised to exercise extreme care in their personal use of social networking sites, considering 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. Staff should not “friend” current or former students under the age of 18.

5. Unacceptable Use

5.1. Appendix 1 provides a list of Dos 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:

5.1.1. 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.

5.1.2. 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.

5.1.3. to access, view, download, post, email or otherwise transmit pornography, sexually suggestive or any other type of offensive, obscene, or discriminatory material.

5.1.4. 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.

5.1.5. 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.

5.1.6. 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;

5.1.7. to collect or store personal information about others without direct reference to The Data Protection Act;

5.1.8. 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;

5.1.9. 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;

5.1.10. to undertake any activity (whether communicating, accessing, viewing, sharing, uploading or downloading) which has negative implications for the safeguarding of children and young people;

5.1.11. Teaching staff must ensure that all film clips are age-appropriate and that there are no inappropriate images or adverts on webpages around the video clip (such as may be found in YouTube pages).

5.2. 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.

5.3. Where an individual accidently or unintentionally accesses a website or material that contains any prohibited content, they must leave the site immediately and inform 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. Genuine mistakes and accidents will not be treated as a breach of this policy.

5.4. 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.

6. Personal and private use

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

6.1.1. taking place at the expense of contracted working hours (i.e., is not taking place during paid working time)

6.1.2. interfering with the individual's work

6.1.3. relating to a personal business interest

6.1.4. involving the use of news groups, chat lines or similar social networking services

6.1.5. at a cost to the school

6.1.6. detrimental to the education or welfare of pupils at the school

6.2. 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.

6.3. 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.

6.4. 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.

6.5. Whilst individuals may be required to use their personal mobile telephone to contact the school, staff should exercise care and seek reimbursement as outlined in section 3.

7. Security and confidentiality

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

7.2. 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.

7.3. 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. Use of portable media should be avoided. 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.

7.4. Where staff are permitted to work on material at home and bring it in to upload to the school server, 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.

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

7.6. 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.

7.7. 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.

7.8. 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.

7.9. 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.

8. Monitoring

8.1. The school is required, as outlined within Keeping Children Safe in Education Legislation, 2023, to monitor internet usage of all ICT users. The school uses and complies with Hampshire Internet and Intranet Policies.

8.2. The school and county council reserve the right to monitor the use of email, internet and intranet communications. The primary tool for this monitoring is the use of the Smoothwall filtering system. Where necessary, data may be accessed or intercepted in the following circumstances:

8.2.1. to ensure that the security of the school and county council's hardware, software, networks and systems are not compromised
8.2.2. to prevent or detect crime or unauthorised use of the school or county council's hardware, software, networks or systems
8.2.3.to gain access to communications where necessary where a user is absent from work
8.2.4 to ensure compliance with Keeping Children Safe in Education legislation

8.3. Where staff have access to the internet during the course of their work or connect personal devices, 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.

8.4. 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.

9. Whistleblowing and cyberbullying

9.1. 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 (DSL).

9.2. 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 (0800 030 5182) and also via the UK Safer Internet Centre helpline@safetinternet.otg.uk or 0844 381 4772.

9.3. Further advice on cyberbullying and harassment can be found in the School Social Media Policy and in Cyber bullying: Practical Advice for School Staff.

10. Signature

10.1. 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.

10.2. 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

Additions to the Hampshire MOPP

1 Guidance to staff on using ICT systems at CPS

10.3. All staff have a home/personal workspace area in which to save their current work. Please keep this area tidy and remove old/unwanted or very large files when not needed. Archive files which are not needed on a regular basis or delete the files if no longer needed. A spot-check of staff home areas is undertaken periodically to monitor content for inappropriate material. Utilise cloud-based storage solutions, including OneDrive.

10.4. SharePoint and Teams are used for shared files and work. Ensure that you place shared files in a location suitable for the right persons to access and remove them when they are not required. Do not place confidential documents in the shared area. The shared area is monitored, and files deleted when they are old. Use cloud-based alternatives where appropriate/possible.

10.4.1. Backups of "private" and "shared" files are kept centrally. If any work goes missing seek support from the ICT technical support team promptly. Staff are encouraged to keep their own backups of archived or important older files, as part of GDPR legislation, we are all required to keep data secure.

2 Roles and Responsibilities

10.4.2. Headteachers and Governors - The Headteachers and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

10.4.3. ICT Technical Support Staff are responsible for ensuring that:

- The IT technical infrastructure is secure
- Anti-virus is fit-for-purpose, up to date and applied to all capable devices.

Windows (or other operating system) updates are regularly monitored, and devices updated as appropriate and kept within supported versions

Any e-Safety technical solutions such as internet filtering are operating correctly.

- Filtering levels are applied age-appropriately.
- Passwords are applied correctly to all users.

3 e-Safety Charter

CPS has a Charter which clearly sets out how the Rights and Responsibilities support all members of the school community including, specifically, students, parents and staff.

3.1.1 Students

- The boundaries of use of ICT equipment and services in school are explained to students in the Acceptable Use Policy. This is signed by students and parents on application for a place at school and is kept on file. Any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.
- e-Safety is embedded into our curriculum; students will be given the appropriate advice and guidance by staff. Similarly, all students will be fully aware how they can report areas of concern whilst at school or outside of school.

3.1.2 Staff

- All staff play a strategic role in supporting students in the correct use of ICT and setting a good example by the way they use ICT themselves.

- Any e-Safety incident is reported to the e-Safety Coordinator, or in their absence to the Headteacher. If there is any uncertainty the matter is to be raised with the e-Safety Coordinator or the Headteacher to make a decision.
- Personal data about staff, students and parents should not be downloaded and stored on devices and personal information must absolutely not be stored on a personal device.

3.1.3 Parents

- Parents play an important role in the development of their children. Through parents' consultation events and communications, the school will keep parents up to date with new and emerging e-Safety risks and will involve parents in strategies to ensure that students are empowered.
- Parents must also understand that the school has rules in place to ensure that their child can be properly safeguarded. Parents will digitally sign the student Acceptable Use Policy before any access can be granted to school ICT equipment or services.

4 e-Safety skills development for staff

- A Digital Wellbeing promotion and newsletter will be published for all staff on a regular basis.
- Staff receive information and training on e-Safety issues.
- New staff receive information on the school's e-Safety policy as part of their induction.
- All staff are made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community
- All staff are encouraged to incorporate e-activities and awareness topics within their curriculum areas.

5 e-Safety taught in the Curriculum

Our children should be educated and coached in order to become safe and respectful 'digital citizens'.

ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-Safety guidance to be given to the students on a regular and meaningful basis. e-Safety is embedded within our curriculum, and we continually look for new opportunities to promote e-Safety.

- The e-Safety policy is introduced to the students early in the Autumn Term each year.
- The school has a framework for teaching internet skills in Computing/ PHSE lessons.
- The school provides opportunities within a range of curriculum areas to teach about e-Safety.
- Educating students on the dangers of technologies that may be encountered outside school is provided when opportunities arise, and as part of the e-Safety curriculum.

- Students are made aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Students are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities.
- Students are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Students are also aware of where to seek advice or help if they experience problems when using the internet and related technologies, i.e. parent, member of staff, an organisation such as Childline, or by using the CEOP report abuse button.

6 Evaluation & Review

The implementation of this policy will be monitored by the Head Teacher, by the Senior Leadership Team and by the Governing Body.

The implementation of this policy will be reviewed, and its impact monitored, in accordance with the Governing Body's programme for Policy Review - refer to CPS-NS-X-PRO-002 Document Review Procedure.

Appendix 1: Cyberbullying Dos and Don'ts from the Hampshire MOPP

Cyber-bullying: Practical Advice For School Staff

The development of new technologies and systems e.g., mobile phones, email and social networking websites means that bullying is often now taking on a new form; cyber-bullying. Victims of cyber-bullying can experience pain and anxiety as much as traditional forms of bullying, particularly as it can occur outside of the school and school hours, significantly intruding into the personal life of the victim. Whilst it is difficult for schools and teachers to deal with this as they have no direct control over external websites there are a range of actions that school staff can take to reduce the chances of cyber-bullying occurring and actions that can be undertaken where it has already occurred.

The guidelines for Headteachers and Governors in dealing with allegations of bullying or harassment define cyberbullying as "the use of information and communication technologies to threaten, harass, humiliate, defame or impersonate". Cyberbullying may involve email, virtual learning environments, chat room, social networking sites, mobile and landline telephones, digital camera images and game and virtual world sites.

This practical advice supplements the guidelines and provides links to other guidance available to school staff in relation to Cyberbullying.

DOs

- Keep passwords confidential
- Ensure you familiarise yourself with your school's policy for acceptable use of technology, the internet, email and HCC and school intranets.
- Ensure any social site you use has restricted access
- Ensure that you understand how any site you use operates and therefore the risks associated with using 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
- Check what images and information is held about you online but undertaking periodic searches of social networking sites and using internet search engines
- Take care when publishing information about yourself and images of yourself online – assume that anything you release will end up in the public domain
- Be aware that any off-duty inappropriate conduct, including publication of inappropriate images and material and inappropriate use of technology could lead to disciplinary action within your employment
- Liaise with your Headteacher and Head/Leader of ICT to remove inappropriate material if it appears on the school website

- Take screen prints and retain text messages, emails or voice mail messages as evidence
- Follow school policies and procedures for e-safety, including access to and use of email, internet and HCC intranet
- Follow school procedures for contacting parents and/or pupils
- Only contact pupils and/or parents via school-based computer systems
- Keep your mobile phone secure at all times
- Answer your mobile telephone with 'Hello' rather than your name, if the number on the display is unknown to you
- Use a school mobile phone where contact with parents and/or pupils has to be made via a mobile (eg during an educational visit off site)
- Erase any parent or pupil data that is stored on a school mobile phone after use
- Seek support from your manager, professional association/trade union, friend, employee support line as necessary
- Report all incidents of cyberbullying arising out of your employment to your Headteacher
- Report any specific incident on a Violent Incident Report (VIR) form as appropriate
- Provide a copy of the evidence with your Headteacher when you report it and further evidence if further incidents arise
- Seek to have offensive online material removed through contact with the site
- Report any threatening or intimidating behaviour to the police for them to investigate
- Access and use the DCSF guidance on Cyberbullying, specifically the advice on reporting abuse and removal of material/blocking the bully's number/email (see attachment/link below)
- Support colleagues who are subject to cyberbullying

DON'Ts

- Allow any cyberbullying to continue by ignoring it and hoping it will go away
- Seek to return emails, telephone calls or messages or retaliate personally to the bullying
- Put information or images online, take information into school, or share them with colleagues, pupils or parents (either on site or off site) when the nature of the material may be controversial
- Accept friendship requests from pupils or parents
- Release your private email address, private phone number or social networking site details to pupils and parents
- Use your mobile phone or personal email address to contact parents and/or pupils
- Release electronically any personal information about pupils except when reporting to parents
- Pretend to be someone else when using electronic communication

- Take pictures of pupils with school equipment without getting parental permission or without being directed to undertake such activity for an appropriate specified purpose
- Take pictures of pupils on your own equipment

The Childnet International have produced a document, "Cyberbullying: Supporting School Staff" which is a useful source of reference to all school staff and leaders. This is linked below:

http://publications.dcsf.gov.uk/default.aspx?PageFunction=productdetails&PageMode=publications&ProductId=DCSF-00242-2009&

Further guidance is available to schools in relation to Cyberbullying as a whole school community and specifically in relation to cyberbullying of and by pupils via:

- www.teachernet.gov.uk
- www.becta.org.uk
- www.digizen.org

Appendix 2: Dos and Don'ts advice for Staff using ICT resources (MOPP guideline)

Dos and Don'ts: Advice for Staff

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 Designated Safeguarding Lead 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, VLEs 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 VLE, school intranet or intranet without prior agreement from a member of senior staff

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 online – 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)

Appendix 3: References

This policy is based on the model policy provided by Hampshire Educational Personnel Services available here: https://www.hants.gov.uk/educationandlearning/education-personnel-services/manual/managing-staff/ict-social-media