STAFF ACCEPTABLE USE OF ICT POLICY

(including School Social Media Policy)

Author: Mrs Valeriia Yemets

Responsibility: Curriculum Committee

Last Updated: September 2024

Review Date: September 2027

This Policy applies to all employees and volunteers 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 volunteers 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 the use is inconsistent with the expectations of staff working with children and young people.

1.0 Access

1.1 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.

1.2 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 are able to access email outside of school hours, the email should be used to undertake school business outside of normal office hours.

1.3 Access to certain software packages and systems (e.g. HCC intranet; SAP, SIMS, RAISE Online, Target Tracker, Schoolcomms) will be restricted to nominated staff and unless permission and access has been provided, staff must not access these systems.

1.4 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.

1.5 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.

1.6 A school mobile phone is available for school trips. If this is not available, staff may use, in urgent or emergency situations during off site visits, their personal mobile telephones. Where used in emergency situations and a cost incurred, the school will provide reimbursement of the cost of the 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 an individual's personal mobile. School staff who have access to colleagues' personal contact details must ensure they are kept confidential.

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

1.8 Staff may have access to the school telephone system. If this facility is used it must be done during break periods, must not be excessive and the length of the call and area phoned if outside the UK should be made known to the school.

1.9 The school will ensure that the Display Screen Equipment assessments are undertaken in accordance with the Health and Safety Policy

2.0 Communication with parents, pupils and governors

2.1 The school communicates with parents and governors through a variety of mechanisms. The points below highlight who is authorised to use which systems and can directly communicate without requiring any approval before use or to agree content:

2.2 School telephones – all teachers, office staff and staff who have been permitted through their roles in pupil welfare. Normally, LSA's and Lunchtime supervisors would need to seek approval from a member of the teaching staff where they feel they need to make a phone call. to a parent.

2.3 School communications via Parentmail (texts and email) are sent out via the school office with authorisation from the Headteacher.

2.4 Letters – All teachers may send letters home but they need to go through the school office first. Where office staff send letters home these will normally be approved by the Finance and Admin Manager and Headteacher.

2.5 Email – school email accounts should not be used for communications with parents. Email can be used as a communication method amongst school governors and the PA.

2.6 Visits home – All home visits are normally subject to approval by the School Leadership and Management Team.

2.7 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.

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

3.0 Social Networking

3.1 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 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.

3.2 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.

3.3 Where school staff do accept friendships via their social networking with ex-pupils aged over 18, they are advised to notify the headteacher.

3.4 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.

3.5 School staff are strongly advised not to accept friendships via their social networking sites 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.

3.6 School staff are able to accept friendships with colleagues via their social networking sites 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.

3.7 If 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.

3.8 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.

4.0 Unacceptable Use

4.1. 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:

4.1.1 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.

4.1.2 to present any personal views and opinions as the views of the school, or to make any concerns that are libellous, slanderous, false or misrepresent others.

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

4.1.4 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.

4.1.5 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.

4.1.6 to intentionally 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.

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

4.1.8 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.

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

4.2 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 Strategic Leadership Team.

4.3 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 Strategic Leadership Team. The school uses Hampshire County Council blocking systems to avoid the potential of this happening. The School Business Manager will report any such unsuitable site the HCC ICT department. Reporting to the Headteachers or Strategic Leadership Team equally applies where school staff are using school equipment at home and accidentally access inappropriate sites or material.

4.4 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 Strategic Leadership Team so that this can be dealt with appropriately.

5.0 Personal and private use.

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

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

5.1.2 interfering with the individual's work

5.1.3 relating to a personal business interest

5.1.4 involving the use of news groups, chat lines or similar networking services

5.1.5 at a cost to the school

5.1.6 detrimental to the education or welfare of pupils at the school

5.2 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.

5.3 Staff should also be aware that inappropriate use of their own personal or other ICT facilities in their personal time, could have implications for their employment situation where it becomes known and the activities undertaken are inconsistent with the expectations of staff working with children.

5.4 Where school staff have brought their own personal equipment such as mobile telephones, digital assistants, laptops and cameras, into 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 own 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.

5.5 Whilst individuals may be required to use their personal mobile telephone to make contact with the school, staff should exercise care and seek reimbursement as outlined in section 1.

6.0 Security and confidentiality

6.1 Any concerns about the security of the ICT system should be raised with a member of the Senior Leadership Team.

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

6.3 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 ICT manager or technician.

6.4 Where staff are permitted to work on material at home and bring it in to upload to the school server through their memory sticks, 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.

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

6.6 Whilst any members of staff may be involved in drafting material for the school website, staff must ensure that they follow appropriate and agreed approval processes. Work must be submitted to the ICT Leader and ICT Technician, who

will seek authorisation from the Headteacher, prior to material being uploaded to the website.

6.7 The ICT Leader and ICT Technician are responsible for ensuring 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.

6.8 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 taking sensitive pupil/staff related data off site and electronic data must only be taken off site in a secure manner, either through password protection on memory sticks or through encrypted memory pens. This is also particularly important when communicating personal data via e mail 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.

6.9 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.

7.0 Monitoring

7.1 The school complies with Hampshire County Council's email, internet and intranet policies.

7.2 The school and the 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:

7.2.1 to ensure that the security of the school and the county council's hardware, software, networks and systems are not compromised.

7.22 to prevent or detect crime or unauthorised use of the school or county council's hardware, software, networks or systems.

7.2.3 to gain access to communications, where necessary, where a user is absent from work.

7.3 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.

7.4 To protect the right of 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 discussion with HCC's HR, ICT and Audit Services and following an assessment to determine whether access or interception is justified.

8.0 Whistleblowing and cyberbullying

8.1 Staff who have concerns about any abusive or inappropriate use of ICT resources, 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 Leads.

8.2 Staff are strongly advised to notify their Headteacher if they are subject to cyberbullying or concerns of e safety. Advice can also be sought from professional associations, trade unions and Hampshire County Council's Employee Support Line (02380 626606). Also via the UK Safer Internet Centre helpline@safeinternet.otg.uk or 0844 381 4772.

9.0 Signature

9.1 Staff are required to read and sign a declaration as outlined in Appendix 2, to confirm they have had access to the acceptable use policy and that they accept and will follow its terms.

9.2 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.

Do's and Don'ts: Advice for Staff Appendix 1

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 quipment 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 unless these are for immediate school use and the images are regularly deleted

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 publish pictures of school pupils online

Don't

- 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 internet 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 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

Staff Code of Conduct for ICT Appendix 2

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with parents, pupils and others, they are asked to sign this code of conduct. Staff should consult the detail of the school's Policy for Staff Acceptable Use of ICT for further information and clarification.

- I appreciate that ICT includes a wide range of system, including mobile phones, personal digital assistants, cameras, email, internet and HCC intranet access and use of social networking and that ICT use may also include personal ICT devices when used for school business
- I understand that it may be a criminal offence to use the school ICT system for a purpose not permitted
- I understand that it I am unable to communicate information which is confidential to the school or which I do not have the authority to share
- I understand that school information systems and hardware may not be used for personal or private without the permission of the Headteacher
- I understand that my use of school information systems, internet and email may be monitored and recorded, subject to the safeguards outlined in the policy to ensure policy compliance
- I understand the level of authority required to communicate with parents and pupils using the various methods of communication
- I understand that I must not use the school ICT system to access inappropriate content
- I understand that accessing, viewing, communicating and downloading material which is pornographic, offensive, defamatory, derogatory, harassing or bullying is inappropriate use of ICT
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager. I will not use anyone's account except my own.
- I will not install any software or hardware without permission
- I will follow the school's policy in respect of downloading and uploading of information and material
- I will ensure that personal data is stored securely and is used appropriately whether in school, taken off the school premises or accessed remotely. I will not routinely keep personal data on removable storage devices. Where personal data is required, it will be password protected/encrypted and removed after use.
- I will respect copyright, intellectual property and data protection rights
- I understand use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.
- I will report any incidences of concern regarding children's safety to the Designated Safeguarding Lead or Headteacher.

- I will report any incidences of inappropriate use or abuse of ICT and inappropriate electronic communications, whether by pupils or colleagues, to the Headteacher, or if appropriate, the Chair of Governors
- I will ensure that any electronic communication undertaken on behalf of the school, including email and instant messaging are compatible with my professional role and that messages do not present personal views or opinions and cannot be misunderstood or misinterpreted
- I understand the school's stance on use of social networking and given my professional role working with children, will exercise care in any personal use of social networking sites
- I will ensure that any electronic communications with pupils, where permitted, are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote e-safety with pupils in my care and help them to develop a responsible attitude to system use, communication and publishing.
- I understand that inappropriate use of personal and other non-school based ICT facilities can have implications for my employment at the school where this becomes known and that activities undertaken are inconsistent with expectations of staff working with children

The school may exercise its right to monitor the use of the school's ICT systems and accesses, to intercept email and to delete inappropriate materials where it believes unauthorised use of the school's ICT systems may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, images or sound.

School Social Media Policy

1 Preamble

1.1 This document should be read in conjunction with information contained in the Model Policy on Staff Acceptable Use of ICT together with the Council's "Guidance on using Social Media" and other related policy documents referred to at Appendix 1 below. Each school will wish to customise the document to match its own specific situation.

1.2 The policy has been developed having regard to guidance provided by the professional associations for teachers and school leaders, other recognised trade unions, and by ACAS. It sets out the rules and standards to be applied for use of the Internet and social media in Hampshire schools. It provides information and guidance for both professional and personal use and outlines the risks to users and schools, as well as the potential consequences of misuse of the Internet and social media.

2 Introduction

2.1 It is recognised that social networking has the potential to play an important part in many aspects of school life, including teaching and learning, external communications and continuing professional development. This policy therefore encourages the responsible and professional use of the Internet and social media to support educational delivery and professional development.

2.2 The Internet provides an increasing range of social media tools that allow users to interact with each other. Whilst recognising the important benefits of these media for new opportunities for communication, this policy sets out the principles that school staff, governors and contractors are required to follow when using social media.

2.3 It is essential that pupils/students, parents and the public at large have confidence in the school's decisions and services. The principles set out in this policy are designed to ensure that staff members use social media responsibly so that confidentiality of students and staff members and the reputation of the school and the County Council are safeguarded. In this context, staff members must be conscious at all times of the need to keep their personal and professional lives separate.

3 Objectives

3.1 The primary objective of this policy is to set out the responsibilities of staff, governors and contractors at the school who use the Internet and social networking sites. It is also aimed at ensuring that the Internet and social media are utilised safely, lawfully and effectively for the successful and economic delivery of school-based services.

4 Scope

4.1 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.

4.2 The policy covers personal use of social media as well as the use of social media for official school purposes, including sites hosted and maintained on behalf of the school. It is acknowledged that there is significant potential for the school to exploit the Internet and social media and that this can bring great advantages. The use of both the Internet and social media is therefore actively encouraged.

4.3 The policy applies to personal webspace such as social networking sites (for example Facebook, MySpace, Yapper), blogs, microblogs such as Twitter, chatrooms, forums, podcasts, open access online encyclopaedias such as Wikipedia, social bookmarking sites such as del.icio.us and content sharing sites such as flickr and YouTube. The internet is a fast moving technology and it is impossible to cover all circumstances or emerging media - the principles set out in this policy must be followed irrespective of the medium.

4.4 This policy provides a structured approach to using the Internet and social media and will ensure that it is effective, lawful and does not compromise the school's reputation, school information or computer systems/networks.

5 Risks

5.1 The school recognises the risks associated with use of the Internet and social media and regulates their use to ensure this does not damage the school, its staff and the people it serves. Principal amongst these risks are:

- cyber bullying by pupils/students;
- access to inappropriate material;
- offending behaviour toward staff members by other staff or pupils/students;
- other misuse by staff including inappropriate personal use;
- inappropriate behaviour, criticism and complaints from external sources;
- loss or theft of personal data;
- virus or other malware (malicious software) infection from infected sites;
- disclosure of confidential information;
- damage to the reputation of the school;
- social engineering attacks - i.e. the act of manipulating people into disclosing confidential material or carrying out certain actions;
- civil or criminal action relating to breaches of legislation;
- staff members openly identifying themselves as school personnel and making disparaging remarks about the school and/or its policies, about other staff members, pupils or other people associated with the school.

6 Applying the Policy

6.1 Responsibilities of staff members

6.1.1 The following principles apply to online participation and set out the standards of behaviour expected of staff members as representatives of the School.

6.1.2 The School has a duty to provide a safe working environment free from bullying and harassment. If a staff member uses any information and/or communications technology, including email and social networking sites, to make reference to people working at or for the School, or people receiving services from the School then any information posted must comply with all relevant professional Codes of Practice and the School's ICT Acceptable Use Policy.

6.2 Using the Internet and social media for approved school purposes

6.2.1 Staff must ensure that they use the Internet sensibly, responsibly and lawfully and that use of the Internet and social media does not compromise school information or computer systems and networks. They must ensure that their use will not adversely affect the school or its business, nor be damaging to the school's reputation and credibility or otherwise violate any school policies. In particular:

- the school's Internet connection is for business use and its use, and use of social networking, must only take place in line with the school's policies;
- when acting with approval on behalf of the school, under no circumstances may staff comment or contribute unless identifying themselves as school staff;
- social media accounts must never be used to conduct school business. Any accounts created for this purpose must link to a school email address. The only exception is the use of professional networks (such as LinkedIn), where it is acceptable to use an account linked to a personal email address in both a professional and personal capacity;
- staff members must report any safeguarding issues they become aware of;
- staff members must not cite or reference pupils/students/parents without approval;
- material published must not risk actions for defamation, or be of an illegal, sexual, discriminatory or offensive nature;
- material published must be truthful, objective, legal, decent and honest;
- material published must not breach copyright;
- any publication must comply with all of the requirements of the Data Protection Act 1998, and must not breach any common law duty of confidentiality, or any right to privacy conferred by the Human Rights Act 1998, or similar duty to protect private information;
- material published must not be for party political purposes or specific campaigning which in whole or part appears to affect public support for a political party;
- material published must not be used for the promotion of personal financial interests, commercial ventures or personal campaigns;

- the tone of any publication must be respectful and professional at all times, and material must not be couched in an abusive, hateful, or otherwise disrespectful manner;
- publication must be in line with school policies;
- if used with pupils/students, staff must ensure that the site's rules and regulations allow the age group to have accounts and that the parents are informed of its use;
- staff members must not use the Internet or social media if doing so could pose a risk (e.g. financial or reputational) to the school, its staff or services or where they do not have the approval from the Senior Leadership Team.

6.3 Personal use of Internet and social media

6.3.1 The school's Internet connection is intended primarily for educational use. There is no right for staff to use the Internet for private use and access can be withdrawn at any time. Where staff members are permitted access via the school's Internet connection:

- the school is not liable for any financial or material loss to an individual user in accessing the Internet for personal use;
- the school will monitor Internet and email use by electronic means, and staff cannot expect privacy when using the school's Internet facility;
- personal Internet search histories and the content of emails sent for personal use will be accessed by staff only according to the Council's Internet, Intranet and Email Monitoring Policy and School's disciplinary procedures, and only then when a legitimate concern has been raised by monitoring processes, legitimate concerns expressed by a colleague, or some other legitimate and objective complaint or incident;
- electronic correspondence will only be intercepted in exceptional circumstances.
- users are not permitted to access, display or download from Internet sites that hold offensive material. Offensive material includes, but is not restricted to, hostile text or images relating to gender, ethnicity, race, sex, sexual orientation, religious or political convictions and disability. The school is the final arbiter on what is or is not offensive material or what is or is not acceptable, permissible or excessive use of the Internet – staff concerned about this should refrain from using the Internet for private matters;
- due to the potential impact on school systems, the use of streaming media such as video (YouTube, BBC iPlayer, Vimeo etc.) or audio (internet radio, Spotify, Google Music etc.) should be kept to a minimum.
- due to the potential impact on school systems, the downloading of media for personal use such as video (YouTube, BBC iPlayer, Vimeo etc.) or audio (internet radio, Spotify, Google Music etc.) is not permitted;
- certain websites will be blocked, but it is a breach of this guide to access any of the following types of site:
  - pornography/Adult /mature content
  - gambling/betting/gaming
  - alcohol/Tobacco

- illegal drugs
- auction sites
- violence/hate/racism
- weapons
- any site engaging in or encouraging illegal activity
- illegal file-sharing sites

- staff members who accidentally or unintentionally access a site containing any prohibited content must leave the site immediately and inform the Stratetgic Leadership Team. Genuine mistakes and accidents will not be treated as breach of this policy;
- staff members may not download software from any source without approval;
- staff members are not permitted to alter or tamper with their PC Internet settings for the purpose of bypassing or attempting to bypass filtering and monitoring procedures unless they have been given express permission to do so by the Headteacher;
- staff members must not communicate personal or confidential information via the Internet/Intranet for any purpose, unless expressly authorised to do so by their Senior Leadership Team;
- users must not create, download, upload or transmit any obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;
- users must not create, download, upload or transmit any defamatory, sexist, racist, offensive or otherwise unlawful images, data or other material;
- users must not create, download, upload or transmit material that is designed or would be likely to annoy, harass, bully, inconvenience or cause anxiety to others;
- users must not create, download, upload or transmit any unsolicited commercial or bulk web mail, chain letters or advertisements;
- users must not download any digital media including music, images, photos and video that would be in breach of copyright or licensing arrangements, or where copyright or ownership cannot be determined;
- the use of file sharing services or software is prohibited for any purpose;
- the use of cloud storage e.g. Google Drive, Dropbox, SkyDrive, iCloud, is not permitted for the storage of sensitive personal data.

6.4 **School reputation and confidentiality**

6.4.1 The school recognises an employee's right to a private life. However the school must also ensure its reputation and confidentiality are protected. Therefore an employee using any ICT away from school, including email and social networking sites must:

- refrain from identifying themselves as working for the school in a way that could have the effect of bringing the school into disrepute
- not express a personal view as a school employee that the school would not want to be associated with

- notify the Strategic Leadership Team immediately if they consider that content posted via any information and communications technology, including emails or social networking sites, conflicts with their role in the school
- not have any unauthorised contact or accept 'friend' requests through social media with any pupil/student unless they are family members;
- exercise caution when having contact or accepting 'friend' requests through social media with parents so as not to compromise the school's reputation or school information;
- not allow interaction through information and communications technology, including emails or social networking sites, to damage relationships with work colleagues in the school and/or partner organisations, pupils/students or parents
- not disclose any data or information about the school, colleagues in the school and/or partner organisations, pupils/students or parents that could breach the Data Protection Act 1998
- not use the Internet or social media in or outside of work to bully or harass other staff or others

6.5 Personal Information

6.5.1 School staff must never give out personal details of others, such as home address and telephone numbers. Staff must handle all personal or sensitive information in line with the school's Data Protection Policies.

6.5.2 With the rise in identity theft and fraud, staff may wish to consider the amount of personal information that they display on personal profiles.

7 Cyber bullying and Harassment

7.1 The use of ICT in relation to Bullying and Harassment

7.1.1 This section should be read in conjunction with the guidance contained in "Cyber-bullying: Practical Advice for School Staff"(Appendix 2). Cyber Bullying and Cyber Harassment, like other forms of bullying and harassment, imply a relationship where an individual has some influence or advantage that is used improperly over another person or persons, where the victim(s) is subjected to a disadvantage or detriment, and where the behaviour is unwarranted and unwelcome to the victim. However, in this case the technological environment has meant that the acts of bullying and harassment now include the use of information and communications technology including email and social networking.

7.1.2 The school will consider it a potential disciplinary matter if users utilise any information and communications technology, including email and social networking sites, in such a way as to bully/harass others in the school or in partner organisations, or pupils/students or parents, whether this takes place during or outside of work. Staff members need to be aware that no matter what the privacy settings on their social media/networking site, inappropriate/derogatory information about a colleague in the school or partner organisations, pupils or parents, can find its way into the public domain even when not intended.

7.1.3 It should be noted that a person does not need to directly experience this form of victimisation in order for it to be classed as cyber bullying/harassment. The fact that a person is unaware that offensive or derogatory comments about them have been placed on websites still fits the criteria of cyber bullying/harassment.

7.1.4 If a staff member receives any threats, abuse or harassment from members of the public through their use of social media then they must report such incidents using the school's procedures.

7.2 Senior Leadership responsibility in relation to Bullying and Harassment

7.2.1 The school owes a duty to take reasonable steps to provide a safe working environment free from bullying and harassment.

7.2.2 For this reason, it is essential that the Strategic Leadership Team take appropriate steps to deal with any incident where it is alleged that a staff member has subjected others to abusive or personally offensive emails, phone calls or content on social networking sites such as Facebook, Twitter, or by any other means.

7.2.3 If a Senior Leader is made aware of such an allegation, the Strategic Leadership Team should deal with it in the same way as any other incident of bullying or harassment in line with school policies, by investigating the allegations promptly and appropriately and providing the victim with appropriate support to demonstrate that the matter is being dealt with seriously.

7.2.4 Senior Leaders should encourage staff to preserve all evidence by not deleting emails, logging phone calls and taking screen-prints of websites. If the incident involves illegal content or contains threats of a physical or sexual nature, the Strategic Leadership team should consider advising the employee that they should inform the police. In the event that such evidence contains indecent images of children, it is an offence to save, send, or alter an image or to show it to anyone else. Therefore, the evidence must be placed in a secure location such as a locked cupboard where others will not be able to see it. In these circumstances the Police should be contacted immediately for advice.

8. Signature

8.1 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 School Social Media Policy and that they accept and will follow its terms.

8.2 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 Social Media may become a matter for police or social care investigations.

Appendix 1

Legal and Policy Framework

The School is committed to ensuring that all staff members provide confidential services that meet the highest standards. All individuals working on behalf of the school are bound by a legal duty of confidence and other laws to protect the confidential information they have access to during the course of their work. Disclosure of confidential information on social media is likely to be a breach of a number of laws and professional Codes of Conduct, including the following:

- Human Rights Act 1998
- Common law duty of confidentiality
- Data Protection Act 1998, and
- Employment Practices Data Protection Code

Confidential information includes, but is not limited to:

- Person-identifiable information, e.g. pupil and employee records protected by the Data Protection Act 1998
- Information divulged in the expectation of confidentiality
- School or County Council business or corporate records containing organisationally or publicly sensitive information
- Any commercially sensitive information such as information relating to commercial proposals or current negotiations, and
- Politically sensitive information.

Staff members should also be aware that other laws relating to libel, defamation, harassment and copyright may apply to information posted on social media, including:

- Libel Act 1843
- Defamation Acts 1952, 1996 and 2013
- Copyright, Designs and Patents Act 1988.
- Protection from Harassment Act 1997
- Criminal Justice and Public Order Act 1994
- Malicious Communications Act 1998
- Communications Act 2003, and
- Equality Act 2010

Related Policies

The Social Media policy should be read in conjunction with other relevant school and County Council policies, procedures and Codes of Conduct including:

- County Council Guidance on using Social Media
- IT Policy on email and internet use
- IT acceptable usage standards
- ICT Acceptable Use Policy for Staff
- Internet and Intranet Monitoring Policy
- Cyber bullying: Practical Advice for School Staff
- Disciplinary Procedures
- Equalities Policy

APPENDIX 2
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 on line – 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, Leader of ICT and ICT Technician 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 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 DfE 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 on-line, 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 e-mail address, private phone number or social networking site details to pupils and parents
- Use your mobile phone or personal e-mail 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 unless they are to be used for authorised blogging purposes and the pictures are removed after upload.

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

I have read and understand the Policy for Staff Acceptable Use of ICT/School Social Media Policy and understand that inappropriate use may be considered to be misconduct or gross misconduct and may, after proper investigation, lead to a disciplinary sanction or dismissal. I understand that if I need any clarification regarding my use of ICT facilities, I can seek such clarification from any member of the Senior Leadership Team.

SIGNED: ……

DATE:……...….

NAME (PRINT): ……