1.0 Introduction

1.1 This policy should be read in conjunction with other relevant school and Council policies, procedures and Codes of Conduct including:

• Social Media Policy

• ICT Policy

• Disciplinary Procedure

1.2 Staff should be given sufficient training and knowledge to be able to recognise and report potential misuse and to enable them to use software and systems as relevant to their role. Staff are encouraged to make use of the resources developed by Childnet (http://www.childnet.com)

1.3 It is not the intention of the policy to try to police every social relationship that governors may have with parents and school staff but about reminding individuals of the importance of appropriate boundaries, including through their social media use.

2.0 Application

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

2.2 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 in the course of the employee or volunteer's work. 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.

3.0 Access

3.1 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.

3.2 Where staff have been provided with a school email address to enable them to perform their role effectively, it will not normally be used to communicate with parents and pupils. Where staff are able to access email outside of schools hours, the email facility should not routinely be used to email parents outside of normal school hours.

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

3.4 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 password protected and 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.

3.5 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.

3.6 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.

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

3.8 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.

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

4.0 Communication with parents, pupils and governors

4.1 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:

4.1.1 School Telephones – all teachers, administrative staff and staff who have been permitted through their roles in pupil welfare or home/school link staff. Normally teaching assistants and lunchtime supervisory staff would need to seek approval from a class teacher where they feel they need to make a telephone call to a parent.

4.1.2 Text System – Office staff. Where, in exceptional circumstances other staff need to send a text, this is normally approved by a member of the Senior Leadership Team.

4.1.3 Letters – Normally all teachers may send letters home, but they may be required to have these approved by the Headteacher before sending. Where office staff send letters home these will normally require approval by the Headteacher.

4.1.4 Email – school email accounts should not routinely be used for communication with parents outside school hours. 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.

4.2 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.

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

5.0 Social Media

5.1 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 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.

5.2 School staff should refer to the school's Social Media Use Policy (appendix A) for further guidance.

6.0 Unacceptable Use

6.1 Appendix B 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:

6.1.1 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

6.1.2 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

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

6.1.4 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

6.1.5 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

6.1.6 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

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

6.1.8 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

6.1.9 to use the school's facilities 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

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

6.2 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.

6.3 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 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.

6.4 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.

7.0 Personal and private use

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

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

7.1.2 interfering with the individual's work

7.1.3 relating to a personal business interest

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

7.1.5 at a cost to the school

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

7.2 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.

7.3 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.

7.4 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.

7.5 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

8.0 Security and confidentiality

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

8.2 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.

8.3 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. Where staff are provided with a memory stick for such activity, to both protect the integrity of the server and to save space, this should be used. All staff must review the appropriateness of the material that they are downloading prior to downloading and are encouraged to do so from known and reputable sites to protect the integrity of the school's systems. Where problems are encountered in downloading material, this should be reported to the school's ICT lead.

8.4 Where staff are permitted to work on material at home they must ensure that it is saved on the Google Drive as this will provide an extra level of virus protection. Staff should not keep any data on USB sticks unless they are fully encrypted. Staff are responsible for ensuring that any USB sticks are virus free and are not connected to any of the school's equipment if infected.

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

8.6 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.

8.7 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.

8.8 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. Communication of data must not be used via ordinary email systems. Staff must ensure that they use

Switch Egress when communicating such data with outside agencies. 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. When communicating such data within school, staff must use the Google Drive due to its encrypted security.

8.9 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.

9.0 Monitoring

9.1 The school uses LGfL and Wandsworth ICT services and therefore is required to comply with their email, internet and intranet policies.

9.2 The school and 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:

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

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

9.2.3 to gain access to communications where necessary where a user is absent from work

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

9.4 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 Dunraven Academy Trust's HR, IT and Audit Services and following an assessment to determine whether access or interception is justified.

10.0 Whistleblowing and cyberbullying

10.1 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).

10.2 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 the UK Safer Internet Centre helpline@safetinternet.otg.uk or 0844 381 4772

10.3 Further advice on cyberbullying and harassment can be found in the School Social Media Policy and within the ICT Policy.

11.0 Remote Access Policy

Goldfinch Primary provides remote access to help support employees with the delivery of the curriculum and for teaching and learning. It is also intended for managing and administering the ICT networks. Use of the school's remote access service implies acceptance of the conditions of use. The school may refuse to extend remote access privileges to any employee or terminate a remote access arrangement at any time.

11.1 Uses of Remote Access Services

The following list is not exhaustive, but sets out broad areas which the school considers to be acceptable use of remote access.

- To gain access to School Information Management System (SIMS)
- To gain access to resources, files and software on the school network
- To administer the school network remotely

11.2 Use of Computers and Equipment

Any computer used to access the school's remote systems must possess anti-virus and anti-spyware programs. These must be updated regularly, at least once a week. The school bears no responsibility if use of the remote access system causes system crashes, or complete or partial data loss on connected computers. Users of remote access are solely responsible for backing up all data before accessing the system. At its discretion, the school will disallow remote access for any computer that proves incapable, for any reason, of working correctly with the remote access system.

11.3 Potential Security Issues

11.3.1 Viruses and malware: When a computer is directly connected to the internet it can be contacted by any other computer also connected to the internet. As a result, there is a risk of exposure to malware that could connect to and potentially compromise that computer, which in turn risks infecting the school's system. For this reason, precautions must be taken to minimise this risk:

- Make sure up-to-date anti-virus software is installed.
- Make sure the latest operating system patches are installed.
- Run a weekly virus scan.
- If a computer has become infected with a virus or other malware, do not use it to remotely access the school's network until the virus has been deleted.
- Turn on phishing filters on web browsers to reduce the risk of phishing attacks.
- Use an anti-spyware program to detect spyware.

11.3.2 Data security: To avoid a risk of confidential information being disclosed to unauthorised third parties:

- Logout of remote access before leaving the computer.
- Wireless network connections must be encrypted using WPA2 or use a cable connection.
- Do not allow any unauthorised person, including family and friends, to use the remote access login or to access files held on the school's network.
- Use a password protected screensaver to prevent anyone gaining access to the computer
- Do not use password storing facilities found in some programs to automatically remember passwords.
- Do not reveal passwords. If for any reason a password is revealed this should be changed immediately.

This policy will ensure that staff are able to access the school network remotely without risk to the security of the system.

12.0 Signature

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

12.2 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. 6 Do's and Don'ts: Advice for Staff Appendix B 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 (DSL) 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 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 email, the internet, VLEs and school Google Drive

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

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 Google Drive

• upload any material onto the school website that doesn't meet style requirements and without approval

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

• exercise caution when accepting friendship requests from parents (advice is to not accept friendships from parents)– you may be giving them access to personal information, and allowing them to contact you inappropriately

• 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

• 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

• 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

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.

9 Dos:

- Keep passwords confidential
- Ensure you familiarise yourself with your school's policy for acceptable use of technology, the internet, email 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 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 Google Drive
- 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 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 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 available at http://www.childnet.com/ufiles/cyberbullying_teachers.pdf.

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 A - Social Media policy

1. Purpose and scope of the policy

1.1 This policy applies to the use of social media for school business and sets out expectations for staff personal use, whether during working hours or at other times. Its purpose is to help staff avoid the potential pitfalls of sharing information on such social media sites and should be read in conjunction with the Staff Acceptable Use of ICT policy. The policy applies at all times whether using school computers or your own device and both when in school or at home.

2. Introduction

2.1 The School recognises that the internet provides unique opportunities for sharing and communicating in both a personal and professional context. Staff are free to use social media such as Facebook, LinkedIn, Twitter, as well as collaborative tools such as blogs and wikis. However, staff should remain mindful of their professional responsibilities and use sound judgement and common sense.

2.2 When communicating with pupils staff should use a school system (such as Google Classroom or email) as this is more appropriate than using social media. If school systems do not meet your needs consult with the IT Manager who can suggest an alternative and provide advice on using the social media platform appropriately.

3. Guiding principles

3.1 Staff are expected to demonstrate a sense of responsibility and in doing so, adhere to the following principles:

3.2 Staff must not communicate with pupils using a personal social media account or add pupils as ‘friends’ or similar or join the same social media groups. Depending on the circumstances, it may also be inappropriate to communicate with parents or add them as ‘friends’.

3.3 Staff should exercise caution when making links with ex-pupils of the school on a personal social media account. Keep in mind that an ex-pupil may also be linked or ‘friends’ with current pupils which (depending on your privacy settings) may expose your personal information or content.

3.4 Staff should ensure that the privacy settings for any personal social media profiles are configured appropriately and limit the amount of information that is publicly available.

3.5 Staff must be mindful of how they present themselves and the school on such media. The private life of an employee at the School may have professional consequences and this must be considered at all times when sharing personal information in this format.

3.6 Staff must not represent personal views as those of the School, nor disclose the views of colleagues or others working with the school (eg management consultants).

3.7 When writing an internet post, staff should remember that this is not a secure form of communication and consider whether the contents would be more appropriate in a private message. While there may be strict privacy controls in place on personal accounts, information could still be copied and shared by others and can easily enter the public domain. For this reason it is always sensible to consider that all information posted online has entered the public domain.

3.8 Staff should protect the privacy of others by omitting personal information from internet posts such as names, email addresses, home or work addresses, phone numbers or other personal information, and it is recommended that the same principles are followed for the user's own personal information.

3.9 Staff must not post anything that may offend, insult or humiliate others, particularly on the basis of their sex, age, race, colour, national origin, religion or belief, sexual orientation, disability, marital status, pregnancy or maternity. Nor must staff post anything that could be interpreted as threatening, intimidating or abusive. Offensive posts or messages may be construed as cyberbullying.

3.10 Staff must not post disparaging or derogatory remarks about colleagues or the School, or its Governors, volunteers, pupils or parents.

3.11 Staff must not use social media in a way which could constitute a breach of any of the School's employment or other policies.

4. Official use of school social media accounts

4.1 As far as possible school IT systems should be used for all official school business, however social media may be used where school systems do not meet specific requirements, for example communications and marketing, alumnae relations or for specific curriculum needs.

4.2 School social media accounts must be kept separate from personal accounts and registered using a school email address.

4.3 School social media account usernames and passwords must be logged with the IT Manager.

4.4 A designated member of staff must be responsible for managing and approving content posted on the social media account, including content or comments that external parties may post.

4.5 Accounts that are no longer used should be deactivated or deleted.

4.6 The School will monitor the use of school social media accounts to check that their use is compliant with school policies.

5. Removing postings

5.1 Staff may be required to remove internet postings which are deemed to constitute a breach of this policy.

6. Breach of Social Media policy

6.1 Failure to comply with this policy may result in an investigation and hearing under the School's disciplinary policy or other appropriate action.

Appendix B - Staff Code of Conduct for ICT

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 Google Drive 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 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 use 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 Child Protection Liaison Officer 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.

iPad Acceptable Use Policy

• The iPad screen is made of glass and is therefore subject to cracking and breaking if misused; never drop or place heavy objects (book, laptops etc) on top of the iPad.

• Only a soft cloth or approved laptop screen cleaning solution is to be used to clean the iPad screen.

• Do not subject the iPad to extreme temperatures.

• Do not store or leave unattended.

• Users may not photograph any other person without that person's consent

• Photographs of children must be in line with Parent Permission forms

• The whereabouts of the iPad should be known at all times.

• It is a user's responsibility to keep their iPad as safe and secure as possible.

• Images of other people may only be made with the permission of the person, or parents of the person, in the photograph.

• Upon returning the iPad to the school, it is the users responsibility to delete all personal materials, including pictures, passwords and e-mails from the device.

• The iPad is a school tool designed to enhance classroom practice. It is not for personal use.

• If the iPad is lost, stolen or damaged, the Computing Co-Ordinator, ICT Technician or Head Teacher must be informed immediately.

I have read and understand the Policy for Staff Acceptable Use of ICT 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): ……