Uplands Primary School Computing Acceptable Use Policy

Date agreed: September 2022
Date for renewal: September 2023

An Acceptable Use Policy sets out the roles, responsibilities and procedures for the acceptable, safe and responsible use of all computing equipment and online technologies (including the Internet, E-mail, web cams, Instant Messaging and other social networking spaces, Virtual Learning Environments, mobile phones and games). This should be read in conjunction with other polices such as: curriculum policy, child protection policy, safeguarding policy, single equality policy, inclusion, behaviour, code of conduct (staff), remote learning, home learning, online policy, use of social media and our anti-bullying policy.

We also adhere to the guidance given in Keeping Children Safe in Education 2022 part two.

Aims

- To ensure the safeguarding of all children and young people within and beyond the school setting by detailing appropriate and acceptable use of all on-line technologies.
- To outline the roles and responsibilities of everyone using school computing equipment, software and online services.
- To ensure adults are clear about procedures for misuse of any online technologies both within and beyond the school setting.
- To develop links with parents/carers and the wider community ensuring input into policies and procedures with continued awareness of benefits and potential issues of online technologies.

Part 1 of this policy reflects the acceptable use terms as stated in the policy provided by Hampshire County Council, and should be read carefully by all school staff before signing the attached agreement and an annual laptop agreement form. Part 2 of the policy reflects responsibilities towards children and covers their responsibility with regards to acceptable usage and online safety.

Part 1

1.0 Introduction

1.1 This policy has been written using the model policy developed on behalf of all Hampshire maintained schools.

1.2 Staff are 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)

2.0 Application

2.1 This policy applies to all employees and volunteers within Uplands Primary School

and in respect of all computing resources and equipment within the school and resources that have been made available to staff for working at home. Computing 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.

2.2 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 computing facilities, where this use is inconsistent with the expectations of staff working with children and young people.

3.0 Access

3.1 Staff are provided with a log on where they are entitled to use the school computing 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 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 schools hours, the email facility should not routinely be used to undertake school business outside of normal office hours. Thought should be given to staff wellbeing when email communications are sent outside of office hours and where possible schedule functions should be used so that emails are sent during office hours.

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

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 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 (through the Multimedia consent form), and that the school's policy in relation to use of pictures, is followed.

3.6 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 and must ensure that they are kept confidential in accordance with General Data Protection Regulation (GDPR) 2018.
The school has two mobile phones which staff should use to contact parents.

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

3.8 Staff may use the school telephone system; when this is done, it must be done during break periods and must not be excessive, unless in the event of an emergency.

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

3.10 Staff will have access to the school's shared resource server to share work and collaborate with others. Any personal intellectual property left on the school's shared resource server once a member of staff leaves becomes the intellectual property of the school itself.

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 a home/school link staff. Normally learning support staff and lunchtime supervisory staff would need to refer a phone call to a member of staff with permission to make telephone calls home or seek approval from a member of the senior leadership team where they feel they need to make a telephone call to a parent.

4.1.2 Text System – Office staff. Where 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 these must be approved by the Headteacher or a Key Stage Leader 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 be used for communication with parents unless approved by a member of the senior leadership team. Email is used as a normal method of communication amongst school governors and where governors are linked in particular areas with members of staff, communication may take place via email.

4.1.5 Visits home – All home visits are normally subject to approval by the senior leadership team and must follow the school's policy on home visits.

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. It must also be scanned by the schools antivirus software before opening.

5.0 Social Networking (In conjunction with the School's social media policy)

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 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.

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

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

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

5.6 Where the school uses social networking sites as a means of communication with the

school community, school staff must follow the guidance provided by the school in the use of the sites.

5.7 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.

6.0 Unacceptable Use

6.1 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:

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 computing 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 computing 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 General Data Protection Regulation (GDPR) 2018

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 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 computing resources including email and the intranet, advice should be sought from a member of the Senior Leadership Team or Computing 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.*

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 computing 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 and are not removed from the school site.

7.5 Whilst individuals may be required to use their personal mobile telephone to make contact with the school, staff should exercise care when doing this.

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 Administration Officer.

8.4 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.

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/newsletter, staff must ensure that they follow appropriate and agreed approval processes before uploading material to the website.

8.7 The school ICT Technician is 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 member of 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 General Data Protection Regulation (GDPR) 2018. 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 sticks or through encrypted memory sticks. This is also particularly important when communicating personal data via email rather than through secure systems. In these circumstances, staff must ensure that they have the correct email address and have verified the identity of the person that they are communicating the data with.

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

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

9.2.1 to ensure that the security of the school and county 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 county 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 or county 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 Hampshire County Council'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 follow school procedure as set out in the Child Protection policy, and alert the Headteacher to such abuse. Where a concern relates to the Headteacher, this should be disclosed to the Chair of Governors or directly to the LADO. If any matter concerns child safety, it should also be reported to the Designated Safeguarding Lead.

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

11.0 Signature

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

11.2 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.

Appendix 1

Do's and Don'ts: Advice for Staff

Whilst the wide range of computing 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 computing 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 computing technology 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 computing 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 General Data Protection Regulation (GDPR) 2018 when using personal data
• seek approval before taking personal data off of the school site
• ensure personal data is stored safely and securely whether kept on site, taken off site or accessed remotely
• report any suspected misuse or concerns that you have regarding the school's systems, resources and equipment to the Headteacher or designated manager and/or Child Protection Liaison Officer as appropriate
• be aware that a breach of your school's Acceptable Use Policy will be a disciplinary matter and in some cases, may lead to dismissal
• ensure that any equipment provided for use at home is not accessed by anyone not approved to use it
• ensure that you have received adequate training in computing
• ensure that your use of computing resources 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 computing 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, Seesaw 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 (Social media and use of digital media policy)
• ensure that you reimburse your school for personal telephone calls as required
• use school mobile telephones when on educational visits
• only use personal mobile devices in the staff room or in classrooms before/after school operating hours and never when pupils are present.

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 personal mobile devices in front of children

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 (Social media and use of digital media policy/ General Data Protection Regulation (GDPR) 2018)
• ensure that parental consent has been given before you take pictures of school pupils (through Multimedia Consent form)

Don't
• bring personal recording equipment into school without the prior approval of the Headteacher
• inappropriately access, view, share or use material recorded other than for the purposes for which it has been recorded
• put material onto the VLE, school intranet or intranet without prior agreement from a member of senior staff

Use of social networking sites

Do
• ensure that you understand how any site you use operates and therefore the risks associated with using the site
• familiarise yourself with the processes for reporting misuse of the site
• ensure that privacy settings on any social media application are at an appropriately high level
• 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 official school based channels of communication

• through your teaching, alert pupils to the risk of potential misuse of social networking sites (where employed in a teaching role)

Don't

• spend access social networking sites during working hours (contact time)
• 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 Computing **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 Computing Acceptable Use Policy for further information and clarification.

I appreciate that computing 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 computing use may also include personal computing devices when used for school business

- I understand that it may be a criminal offence to use the school computing 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 comptuing 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 computing resources is not allowed and doing so will result in disciplinary action
- 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 computing resources 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 online safety with pupils in my care and help them to develop a responsible attitude to system use, communication and publishing (in line with the school's Online Safety policy).
- I understand that inappropriate use of personal and other non-school based computing 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 computing systems and accesses, to intercept email and to delete inappropriate materials where it believes unauthorised use of the school's computing 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.

I have read and understand the Computing Acceptable Use Policy and I 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 computing facilities, I can seek such clarification from any member of the Senior Leadership Team. I agree to adhere to this policy.

SIGNED: ……

DATE:……..….

NAME (PRINT): ……

Part 2

The following part of the policy describes the responsibilities towards the children and learning. Within this section, references to the Virtual Learning Environment (VLE) apply to all ICT equipment and software, including email, the school's website and any VLE/learning platform software currently in use.

School responsibilities

- To provide each pupil with a secure online logon where they can access appropriate materials which are either created or selected by other school members for them.
- To work towards providing every parent with an online secure logon where they can access information about their child's tasks.
- To provide everyone who works with children in the school (and who has been police checked), online access to areas where they can create materials that will help Uplands pupils both educationally and socially.
- To provide Hampshire County Council secure access to school data via SIMS (Schools Information Management Systems) for the purpose of keeping user areas regularly updated.
- To work towards establishing a clear minimum entitlement that each pupil can expect from online learning platforms whilst respecting staff work life balance and the need for pupils to maintain a physically active lifestyle.
- To ensure that only those vetted for working with children have access to Uplands pupils via any Virtual learning environments (VLE). The exception will be parents who may have access to learning platforms such as 'Tapestry' but will only have access to their own children's database, log on and work.
- To ensure the acceptable use policy is shared with children at an age appropriate level and that the children's consent is recorded.

Pupil responsibilities are presented as a series of simple I will statements that can be easily remembered. These will be taught alongside a comprehensive web safety curriculum. See the ICT policy and Key Stage 1 and 2 child friendly rules for online use.

- ✓ I will only use computing in school for school purposes.
- ✓ I will only use my class email address or my own school email address when emailing.
- ✓ I will only open email attachments from people I know, or who my teacher has approved.
- ✓ I will not tell other people my computing passwords.
- ✓ I will only open/delete my own files.
- ✓ I will make sure that all online contact with other children and adults is responsible, polite and sensible.
- ✓ I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this, I will tell my teacher immediately.
- ✓ I will not give out my own details such as my name, phone number or home address.
- ✓ I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- ✓ I will be responsible for my behaviour when using computing resources because I know that these rules are to keep me safe.
- ✓ I know that my use of computing equipment can be checked and that my parent/ carer contacted if a member of school staff is concerned about my safety online.
- ✓ I will follow the rules for using the internet and other computing equipment safely.

Staff responsibilities

- Staff will keep the same level of professional relationship that is observed within school on virtual learning environments.
- Staff will observe best copyright practice
- Staff will endeavour to learn how to make the best use of any learning platforms whilst observing a reasonable work life balance.
- Staff who have a teaching responsibility will endeavour to find the best balance for using learning platforms that reflects our instant modern e-learning culture whilst retaining the best of older teaching methods.
- Staff will respect all intellectual property rights of people who create online resources. Using and adapting these for their pupils but not republishing them outside the school as their own work.
- As in the classroom, teachers are responsible for monitoring submissions by students to 'Mathletics' and other online environments that they have initiated.
- Staff will ensure that any computing resources that are used in the classroom (such as YouTube clips) are suitable to the age of the children they teach, and are only accessible on secure (password protected) teacher laptops.
- Staff will not transfer personal data such as reports, Pen Portraits and contact information on to personal devices unless strictly necessary. This data should then be used in line with General Data Protection Regulation (GDPR) 2018.

Each child or young person will have the Acceptable Use Rules shared with them on an annual basis within school.

Misuse

Uplands takes misuse of any Virtual learning Environment (including the website, emailing system, etc…) by any member of the school community seriously and will deal with any incidents that occur as if they had happened on school property during the school day. Uplands takes the view that all users using the Virtual Learning Environment do so under the direct code of conduct set out here and Hampshire County Councils Acceptable Use policy which can be found on the County Intranet.

Specific Areas of Misuse

NB any form of media refers to text, digital image of any type, video and audio file in the rest of this document

- It is an offence under the schools code of conduct for any member of the school community to publish any derogatory remark in any form of media on the schools Virtual learning Environment.
- It is an offence under the schools code of conduct for any member of the school community to extract any form of media from the Virtual Learning environment for use in cyber bullying outside the schools Virtual Learning environment.
- It is an offence under the schools code of conduct for any member of the school community to publish or store any sexist, racist or sexually exploitative material in any form of media on the Virtual learning environment.

- It is an offence under the schools code of conduct for any member of the school community to knowingly store or seek to spread a virus using the schools Virtual Learning Environment.
- It is an offence under the schools code of conduct for any member of the school community to run a business using the Virtual Learning Environment.

Dealing with Misuse

- To deal with any incidents of cyber bullying that occur on the VLE as if the bullying had taken place within the physical bounds of the school.
- To investigate and work with all parties in any incidents of cyber bullying that take place outside of the VLE between members of the school community where clear evidence is provided. The school takes the position that as these persons would never have met without the school as contact point then the school has a duty to help. Following best practise where cyber bullying threatens violence or is of a sexual nature the police will be asked for their advice/involvement.
- Peer to peer abuse or sharing of inappropriate content or images will be dealt with in line with our behaviour and child protection policies.
- Offences will be dealt with according to the level of the offence in line with school discipline for pupils and guidelines for staff disciplinary procedures. If the offence is a breach of criminal law, the police will be called in and all evidence will be preserved to the best of the schools ability. If the offence is committed by a person not employed by Uplands who has access to the Virtual Learning Environment the Headteacher will decide how to deal with the offence according to best practice.
- Pupil minor infringements of these rules can be dealt with by a withdrawal of certain Virtual Learning Environment privileges such as
    - Withdrawal of ability to message other pupils for a fixed period of time, often 2 weeks for a minor first offence (Pupil would still be able to message teachers)
    - Withdrawal from the whole school group which has access to a whole school chat and whole school discussion forums for a fixed period of time often 2 weeks for a minor first offence.
- As a general principle pupils would not be withdrawn from Virtual learning work areas unless there was extremely good reasons to do so that were in the best interests of the child. Pupils have a right to access the schools virtual learning environment as they have a right to access education through more traditional forms.
- If a pupil is temporarily excluded from the school their Virtual Learning Access would not be removed unless it was in their best interest or in the best interests of other pupils within the school.

Acceptable Use Agreement (Part 2): Staff, Governors and Visitors

Staff, Governor and Visitor

Acceptable Use Agreement / Code of Conduct

Computing resources and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Mrs S Ackerman.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the computing system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
- I will not install any hardware of software without permission of the Computing Technician
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school (including that on social media), will not bring my professional role into disrepute.
- I will support and promote the school's Online Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature …… Date ……

Full Name ……..(printed)

Job title . . . . . .

Online Safety rules

Acceptable Use Agreement:

Pupils – in Key Stage One

KS1 Pupil Acceptable Use

Agreement / eSafety Rules

- ✓ I will not tell other people my computing passwords.
- ✓ I will make sure that all online contact with other children and adults is kind and polite.
- ✓ I will not send or save anything nasty and if I see anything unpleasant I will tell the teacher.
- ✓ I will not give out my own details such as my name, phone number or home address.
- ✓ I will be responsible for my behaviour when using computing resources because I know that these rules are to keep me safe.
- ✓ I know that my use of computing equipment can be checked by my teacher.

Online Safety rules

Acceptable Use Agreement:

Pupils – in Key Stage Two

KS2 Pupil Acceptable Use

Agreement / eSafety Rules

- ✓ I will only use computing resources in school for school purposes.
- ✓ I will only open email attachments from people I know, or who my teacher has approved.
- ✓ I will not send website links to other pupils.
- ✓ I will not send email attachments to other pupils.
- ✓ I will not tell other people my computing passwords.
- ✓ I will only open/delete my own files.
- ✓ I will make sure that all online contact with other children and adults is responsible, polite and sensible.
- ✓ I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- ✓ I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- ✓ I will be responsible for my behaviour when using computing equipment because I know that these rules are to keep me safe.
- ✓ I know that my use of computing equipment can be checked and that my parent/ carer contacted if a member of school staff is concerned about my Online Safety or my actions.