SCHOOL E-SAFETY POLICY

1. INTRODUCTION

1.1 The internet and e-mail play an essential role in the conduct of our business in school. The systems within school are made available to students, teaching staff, support staff and other authorised persons to further enhance both educational and professional activities including teaching, research, administration and management. We value the ability to communicate with colleagues, pupils and business contacts. There has been a substantial investment in information technology and communications (ICT) systems which enable us to work more efficiently and effectively.

1.2 How we communicate with people not only reflects on us as individuals but on the School. Therefore, although we respect your personal autonomy and privacy, we have established this policy to ensure that you know what we expect from you and what you can expect from us in your use of e-mail and the internet.

1.3 We trust you to use the ICT facilities sensibly, professionally, lawfully, consistent with your duties, with respect for your colleagues and in accordance with this Policy.

1.4 For your safety, we are able to monitor all web pages visited, email sent and received, this helps us monitor inappropriate use, such as bullying.

1.5 This policy applies to you as an employee whatever your position, whether you are a Head Teacher, Teacher, support staff,

permanent, temporary or otherwise. Any inappropriate use of the School's internet & e-mail systems whether under this policy or otherwise may lead to disciplinary action being taken against you under the appropriate disciplinary procedures which may include summary dismissal.

1.6 It is important that you read this policy carefully. If there is anything that you do not understand, please discuss it with the Head Teacher or your line manager. Once you have read and understood this policy thoroughly, you should sign this document, retain a copy for your own records and return the original to the Head Teacher

2. GENERAL PRINCIPLES AND LEGAL ISSUES

2.1 All information relating to our pupils, parents and staff is confidential. You must treat all School information with the utmost care whether held on paper or electronically.

2.2 Care must be taken when using e-mail as a means of communication as all expressions of fact, intention or opinion may implicate you and/or the school. Electronic information can be produced in court in the same way as oral or written statements.

2.3 We trust you to use the internet sensibly. Please be aware at all times that when visiting an internet site the unique address for the computer you are using (the IP address) can be logged by the site you visit, thus identifying your school.

2.4 The main advantage of the internet and e-mail is that they provide routes to access and disseminate information. However the same principles apply to information exchanged electronically in

this way as apply to any other means of communication. For example, sending defamatory, sexist or racist jokes or other unsuitable material via the internet or email system is grounds for an action for defamation, harassment or incitement to racial hatred in the same way as making such comments verbally or in writing.

2.5 Internet and e-mail access is intended to be used for school business or professional development, any personal use is subject to the same terms and conditions and should be with the agreement of your head teacher.

2.6 As an employee, you should exercise due care when collecting, processing or disclosing any personal data and only process personal data on behalf of the School where it is necessary for your duties. The processing of personal data is governed by the Data Protection Act 1998. Schools are defined in law as separate legal entities for the purposes of complying with the Data Protection Act. Therefore, it is the responsibility of the School, and not the Local Authority, to ensure that compliance is achieved.

2.7 All aspects of communication are protected by intellectual property rights which might be infringed by copying. Downloading, copying, possessing and distributing material from the internet may be an infringement of copyright or other intellectual property rights.

3. MONITORING COMMUNICATIONS

3.1 This policy takes into account legislation which aims to ensure a minimum level of personal privacy for employees in their employment. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 allows for interception of "business" communications for business purposes:

3.1.1 to establish the existence of facts

3.1.2 to ascertain compliance with applicable regulatory or self regulatory practices or procedures.

3.1.3 to ascertain or demonstrate effective system operation technically and by users.

3.1.4 for national security/crime prevention or detection.

3.1.5 for confidential counselling/support services.

3.1.6 for Investigating or detecting unauthorised use of the system

3.1.7 for monitoring communications for the purpose of determining whether they are communications relevant to the business.

3.2 Research Machines (RM) has a contractual obligation to monitor the use of the internet and e-mail services provided as part of DGfL, in accordance with the above Regulations. Traffic data and usage information may be recorded and may be used in disciplinary procedures if necessary. RM, Dudley MBC and the school reserve the right to disclose any information they deem necessary to satisfy any applicable law, regulation, legal process or governmental request. If there is any evidence that this particular policy is being abused by individuals, we reserve the

right to withdraw from employees the facility to send and receive electronic communications

3.3 If the email is personal, it is good practice to use the word 'personal' in the subject header and the footer text should indicate if it is a personal email the school does not accept responsibility for any agreement the user may be entering into.

3.4 Your privacy and autonomy in your business communications will be respected. However, in certain circumstances it may be necessary to access and record your communications for the School's business purposes which include the following:

3.4.1 providing evidence of business transactions;

3.4.2 making sure the School's business procedures are adhered to;

3.4.3 training and monitoring standards of service;

3.4.4 preventing or detecting unauthorised use of the communications systems or criminal activities;

3.4.5 maintaining the effective operation of communication systems.

4. USE OF INTERNET AND INTRANET

4.1 When entering an internet site, always read and comply with the terms and conditions governing its use.

4.2 Do not download any images, text or material which is copyright protected without the appropriate authorisation.

4.3 Do not download any images, text or material which is inappropriate or likely to cause offence.

4.4 If you want to download any software, first seek permission from the Head Teacher, ICT Coordinator or RM. They should check that the source is safe and appropriately licensed.

4.5 If you are involved in creating, amending or deleting school web pages or content on our web sites(including Portal), such actions should be consistent with your responsibilities and be in the best interests of the School.

4.6 You are expressly prohibited from:

4.6.1 introducing packet-sniffing software (i.e. software which is used to intercept data on a network) or password detecting software;

4.6.2 seeking to gain access to restricted areas of the network;

4.6.3 knowingly seeking to access data which you are not authorised to view;

4.6.4 introducing any form of computer viruses; and

4.6.5 carrying out other hacking activities.

4.7 For your information, the following activities are criminal offences under the Computer Misuse Act 1990:

4.7.1 unauthorised access to computer material i.e. hacking;

4.7.2 unauthorised modification of computer material; and

4.7.3 unauthorised access with intent to commit/facilitate the commission of further offences.

Counter Terrorism and Security Act 2015

The Counter Terrorism and Security Act 2015 was published on 12th March 2015. Section 26 of the Act places a duty on schools in England (and Wales) to prevent people being drawn into terrorism. This duty applies to all schools, whether publicly-funded or independent, and organisations covered by the Early Years Foundation Stage framework. The duty also applies to children's

homes. Statutory guidance has been published and comes into force on 1st July 2015.

4.8 As a school we must be proactive in monitoring risks and be ready to deal appropriately with issues which arise through;

– understanding the nature of the threat from violent extremism and how this may impact directly or indirectly on the school,

– understanding and managing potential risks within the school and from external influences,

– responding appropriately to events in the local, national or international news that may impact on pupils and communities,

– promoting effective ICT security and responsible user policies.

5. USE OF ELECTRONIC MAIL

5.1 You should agree with recipients that the use of e-mail is an acceptable form of communication. If the material is confidential, privileged, or sensitive you should be aware that un-encrypted e-mail is not secure.

5.2 Do not send sensitive personal data via email unless you are using a secure site or portal. It is good practice to indicate that the email is 'Confidential@ in the subject line

5.3 Copies of emails with any attachments sent to or received from parents should be saved in a suitable secure directory or printed copies kept as a secure record.

5.4 Do not impersonate any other person when using e-mail or amend any messages received.

5.5 It is good practice to re-read e-mail before sending them as external e-mail cannot be retrieved once they have been sent.

5.6 Email for students:

This is restricted to KS2 year groups only. Children are only able to communicate with others inside of this establishment. All external/web accessed email accounts are prohibited and should be filtered. Please inform the ICT coordinator or technician if this is not the case.

Content of emails received by children is monitored and any suspicions of radicalisation of extremism must be reported to the Head Teacher immediately!

6. DATA PROTECTION

6.1 Through your work personal data will come into your knowledge, possession or control. In relation to such personal data whether you are working at the School*'s* premises or working remotely you must:

6.1.1 keep the data private and confidential and you must not disclose information to any other person unless authorised to do so. If in doubt ask your Head Teacher or line manager;

6.1.2 familiarise yourself with the provisions of the Data Protection Act 1998 and comply with its provisions;

6.1.3 familiarise yourself with all appropriate School policies and procedures;

6.1.4 not make personal or other inappropriate remarks about staff, pupils, parents or colleagues on manual files or computer records. The individuals have the right to see all information the School holds on them subject to any exemptions that may apply.

6.2 The School views any breach of the Data Protection Act 1998 as gross misconduct which may lead to summary dismissal under appropriate disciplinary procedures.

6.3 **If you make or encourage another person to make an unauthorised disclosure knowingly or recklessly you may be held criminally liable.**

7. Mobile devices for staff members:

7.1.1 **These devices are school property and must be used in accordance with the above policies and procedures.**

7.1.2 **Personal use of these devices is not recommended, however this is taken at the users own risk.**

7.1.3 **It is not advisable to send personal emails from your device unless an individual email account has been added. Otherwise these emails will be reviewable as mentioned in point 3.**

7.1.4 **A secure lock-screen password must be present on any mobile device.**

7.1.5 **Staff members are required to sign a disclosure before being allocated any mobile device.**

7.1.6 **These mobile devices need to be present in school each day as routine maintenance may be required with little notice.**

7.1.7 **Access to network content from home needs to adhere to point 6 above.**

I have read through and fully understand the terms of the policy. I also understand that the School may amend this policy from time to time and that I will be issued with an amended copy.

Signed:……

PRINT NAME……

Dated: ……..

Priority Points for Ham Dingle Primary School:

It is our responsibility to protect the children in our care. Any data, including photos, must be stored securely on the school server and not on mobile storage devices unless encrypted. (Encrypted USB memory sticks are available from the ICT Coordinator.)

Access to such data is no longer exclusive to computers on the School's site. With the addition of CC4Anywhere and Unify, school data and resources are accessible from any internet connected device. Password encryption is the only defence in place to keep this data safe.

Passwords need to be secure, for all members of staff, to ensure no unauthorised users can gain access to school data. Passwords are to be kept private, if you feel your password has been compromised it must be changed. Your ICT coordinator or technician can assist you in checking the security level of your chosen password.

It is our wish to be treated as professionals; therefore we must portray ourselves as professionals in all public domains. Social networking sites are a great advance in electronically sharing and communicating, however, as professionals, with such a responsibility as looking after children, we must make every effort to maintain our professionalism and not leave ourselves vulnerable. It is advised that any users of such sites do not comment on any matter linked to their profession. Any misuse of Social networking must be reported to the Local Authority.