Dormston
SCHOOL
Respect | Commit | Achieve

DORMSTON SCHOOL

Staff Acceptable Use Policy (July 2016)

Rules for Responsible Internet Use

This policy applies to all adult users of the schools systems. 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.

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 the overall acknowledgement slip and return to Jayne Elliott or Steve Dixon.

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. Electronic information can be produced in court in the same way as oral or written statements. You may also be personally liable to prosecution. Please remember that access is a privilege, not a right and inappropriate use may result in that privilege being withdrawn.

Research Machines (RM) has a contractual obligation to monitor the use of the internet and e-mail services provided as part of DGfL, in line with The Telecommunications Regulations 2000. 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.

All information relating to our pupils, parents and staff is confidential (please refer to the school's Data Protection Policy). You must treat all school information with the utmost care whether held on paper or electronically.

Use of the Internet and Intranet

When entering an internet site, always read and comply with the terms and conditions governing its use. 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. For your information, the following activities are criminal offences under the Computer Misuse Act 1990:

- ✓ unauthorised access to computer material i.e. hacking;
- ✓ unauthorised modification of computer material;
- ✓ unauthorised access with intent to commit/facilitate the commission of further offences.

In line with this policy, the following statements apply:-

- ✓ If you download any image, text or material check if it is copyright protected. If it is then follow the school procedure for using copyright material;
- ✓ do not download any image, text or material which is inappropriate or likely to cause offence. If this happens accidentally report it to a senior member of staff;
- ✓ if you want to download any software, first seek permission from the Head Teacher and/or member of staff responsible/RM. They should check that the source is safe and appropriately licensed;
- ✓ if you are involved in creating, amending or deleting web pages or content on the web site, such actions should be consistent with your responsibilities and be in the best interests of the School.

You should not:

- ✓ introduce packet-sniffing software (i.e. software which is used to intercept data on a network) or password detecting software;
- ✓ seek to gain access to restricted areas of the network;
- ✓ knowingly seek to access data which you are not authorised to view;
- ✓ introduce any form of computer viruses;
- ✓ carry out other hacking activities.

Electronic Mail

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. If in doubt please ask yourself the question "does this information (which may be confidential) need to be sent via email – or is another method more secure/appropriate"?

Please be aware that the recipient of your email may not have the same degree of security as the school system. Also be careful when responding with 'reply all'. This may not be appropriate.
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. 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:

- ✓ providing evidence of business transactions;

- ✓ making sure the School's business procedures are adhered to;
- ✓ training and monitoring standards of service;
- ✓ preventing or detecting unauthorised use of the communications systems or criminal activities;
- ✓ maintaining the effective operation of communication systems.

In line with this policy the following statements apply:-

- ✓ 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;
- ✓ 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;
- ✓ copies of emails with any attachments sent to or received from parents should be saved in a suitable secure directory;
- ✓ do not impersonate any other person when using e-mail or amend any messages received;
- ✓ 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;
- ✓ it is good practice to re-read e-mail before sending them as external e-mail cannot be retrieved once they have been sent;
- ✓ 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;
- ✓ 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 the Headteacher;
- ✓ 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.
- ✓ do not use pupils' full names in the subject box and please refrain from opening emails on the interactive whiteboard screens.

Social Networking

The use of social networking sites for business and personal use is increasing. Access to social networking sites are generally blocked by the school systems, however a school can manage access by un-filtering specific sites, internet usage is still monitored.

School staff may need to request access to social networking sites for a number of reasons including:

- ✓ advertising the school or managing an 'official' school presence;
- ✓ monitoring and viewing activities on other sites;
- ✓ communication with specific groups of adult users e.g. a parent group.

Social networking applications include but are not limited to:

- ✓ blogs;
- ✓ any online discussion forums, including professional forums;
- ✓ collaborative spaces such as Wikipedia;
- ✓ media sharing services e.g. YouTube, Flicker;
- ✓ 'Microblogging' applications e.g. Twitter.

Staff are advised to exercise caution when using their own social networking sites, and be aware that if security settings are not set appropriately access may be gained by members of the public. This also applies to postings that you may make on other social networking members' sites.

When using school approved social networking sites the following statements apply:-

- ✓ school equipment should not be used for any personal social networking use;
- ✓ staff must be aware of, and if necessary refer to the school's Child Protection Policy on the network;
- ✓ staff must not accept *friendships* on social networking sites from pupils.
- ✓ Dormston School recommends that no friendship requests are made with past students for at least five years.
- ✓ it is important to ensure that members of the public and other users know when a social networking application is being used for official school business. Staff must use only their @dormston.dudley.sch.uk email address or other school approved email mechanism and ensure all contributions are professional and uphold the reputation of the school;
- ✓ social networking applications should not be used to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claims for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the school into disrepute;
- ✓ postings should not be critical or abusive towards the school, staff, pupils or parents or used to place a pupil, student or vulnerable adult at risk of harm;
- ✓ postings should not site your place of work or events that are occurring;
- ✓ the social networking site should not be used for the promotion of personal financial interests, commercial ventures or personal campaigns, or in an abusive or hateful way;
- ✓ ensure that the appropriate privacy levels are set. Consider the privacy and safety settings available across all aspects of the service - including photos, blog entries and image galleries. Failing to set appropriate privacy levels could result in messages which are defamatory, libellous or obscene appearing on your profile before you have chance to remove them;
- ✓ chat activities take up valuable resources which could be used by others to benefit their studies, and you can never be sure who you are really talking to. For these reasons chat rooms should be avoided.
- ✓ it should not breach the school's Information Security policy.

Data Protection

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.

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. The main advantage of the internet and e-mail is that they provide routes to access and disseminate information.

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:-

- ✓ 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;
- ✓ familiarise yourself with the provisions of the Data Protection Act 1998 and comply with its provisions;
- ✓ familiarise yourself with all appropriate school policies and procedures;
- ✓ do 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.

Individual members of staff can be personally liable in law under the terms of the Data Protection Acts. They may also be subject to claims for damages from persons who believe that they have been harmed as a result of inaccuracy, unauthorized use or disclosure of their data. A deliberate breach of this Data Protection Policy will be treated as a disciplinary matter, and serious breaches could lead to dismissal.

Data held about individuals will not be kept for longer than necessary for the purposes registered. It is the duty of staff to ensure that obsolete data are properly erased.

The School will, in general, only disclose data about individuals with their consent. However there are circumstances under which the School's authorized officer may need to disclose data without explicit consent for that occasion.

- ✓ No memory sticks are to be used to store ANY personal data or data that can be deemed to hold any sensitive materials, i.e. Names, addresses, medical issues etc. If staff are deemed to have effected a breach of policy you may be personally prosecuted for this offence with disciplinary action following.

All staff are advised NOT to use memory sticks at all but use the schools protected area for sensitive data, however encrypted memory devices are available for staff use under certain circumstances. All equipment that holds data must be password controlled in case a third party gets hold of the equipment. If any data or equipment with data on is lost or stolen this must be reported to the data controller as soon as possible.

Review Officer - Simon Carroll
Review Date - September 2017

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

Use of personal mobile phones at school

Please do not use mobile phones during contact time, unless by prior arrangement with the Head Teacher.

I have read through, fully understand and agree to abide by the terms of the policy. I also understand that the school will need to amend this policy periodically and that I will be issued with an amended copy.