ARTHUR MELLOWS VILLAGE COLLEGE

STAFF ICT POLICIES

Presented to:

Governors: Personnel Committee
Tuesday 3 March 2015

Consultation Process	
For review and consideration at Governors’ Personnel Committee	6 March 2012 Approved 6 March 2012
Governors’ Personnel Committee	3 March 2015
Date approved	3 March 2015
Date reviewed	3 March 2015

ARTHUR MELLOWS VILLAGE COLLEGE

STAFF ICT POLICIES

The **Staff ICT Policies** are a collection of 5 individual policies which cover the use of the network, use of non-domain devices, use of the internet, use of the College's email system and use of data.

CONTENTS

1.0 NETWORK ACCEPTABLE USE POLICY

1.1 The College reserves the right to monitor staff desktop/laptop usage*.

1.2 No third party software must be in installed on any desktop/laptop without the consent of the ICT Manager**.

1.3 Staff will take responsibility for all activity that takes place under their own login.

1.4 All users should make themselves familiar with the College's **Display Screen Equipment (DSE) Policy** prior to using any ICT equipment.

1.5 All users should make themselves familiar with the College's **Data Protection Policy**.

1.6 Any ICT problems/issues should be reported to the IT Department immediately.

1.7 Any breach of the Network Acceptable Use Policy will be dealt with in accordance with the College's disciplinary rules and Disciplinary Policy.

* No monitoring software is installed on IT or SMT staff desktop/laptops.
** Software to enable the use of home internet services may be installed without prior permission.

NETWORK ACCEPTABLE USE POLICY

ICT resources should not be used for anything other than College business with the exception of the internet†, email††, letters of application/CV and other professional matters.

Only the network account holder is permitted to use that network account.

Passwords are to be kept confidential.

Individually issued staff laptops must not be used by non College employees.

Unattended laptops must be left in a locked room/office. Where security equipment is provided it must be used.

Laptops must not be left unattended in a vehicle at any time.

Print outs must be kept to a minimum. Multiple copies should be produced via Reprographics.

Staff must not attempt to disable or remove the monitoring software on any machine.

Staff must not attempt to disable or remove the virus checker software on any machine.

The use of ICT resources for any illegal purpose is forbidden.

†Personal use permitted under the conditions of the **Internet Acceptable Use Policy**
††Personal use permitted under the conditions of the **Email Acceptable Use Policy**

2.0 INTERNET ACCEPTABLE USE POLICY

2.1 The College reserves the right to monitor staff internet usage.

2.2 Staff are permitted to wirelessly connect to the internet using their own personally owned devices, such as smartphones and tablets.

2.3 Staff will take responsibility for any sites visited or content viewed using the internet.

2.4 The College accepts no liability for any personal financial transactions which are made across the internet.

2.5 Where inappropriate sites are identified by accident the ICT Department should be informed immediately.

2.6 Any breach of the **Internet Acceptable Use Policy** may result in the loss of internet access.

INTERNET ACCEPTABLE USE POLICY

Personal use of the internet is permitted, except in curriculum areas during normal school hours and at all times when students are present in the room.

The use of chat rooms is not allowed.

The use of the internet for betting and/or gambling is forbidden.

The use of the internet for personal financial gain is forbidden.

The use of the internet for advertising purposes is forbidden.

The use of the internet for political purposes is forbidden.

The use of the internet for any illegal purpose is forbidden.

The viewing / downloading of racist, pornographic, sexist or obscene material is not permitted.

The posting of anonymous messages via the internet is not permitted.

The copyright and intellectual property rights of all content viewed / downloaded must be respected.

3.0 EMAIL ACCEPTABLE USE POLICY

3.1 The College reserves the right to monitor email and any associated electronic attachments.

3.2 Staff will take responsibility for the content of any email sent.

3.3 The College accepts no liability for any personal financial transactions which are made via email.

3.4 Staff should note that emails can be as legally binding as a written letter.

3.5 Staff should beware of emails and/or attachments from unknown sources. If in doubt, delete immediately. Do not open any suspicious message(s).

3.6 Non-required emails and attachments should be deleted once read.

3.7 All emails sent externally will be automatically appended with the following disclaimer: ***This message is private and confidential. If you have received this message in error, please notify us and remove it from your system.***

3.8 Any breach of the **Email Acceptable Use Policy** may result in the loss of email access.

EMAIL ACCEPTABLE USE POLICY

Email is provided primarily for business use, excessive personal use is not permitted.

Requests for mailing lists or similar services should be made for College business purposes only.

Nothing should be sent via email that could tarnish the College's name or expose it to legal action.

The use of email for betting and/or gambling is forbidden.

The use of email for personal financial gain is forbidden.

The use of email for advertising purposes is forbidden.

The use of email for political purposes is forbidden.

The use of email for any illegal purpose is forbidden.

The use of email to send libellous, slanderous, threatening or abusive messages is forbidden.

The use of email for the viewing / transmission of racist, pornographic, sexist or obscene material is not permitted.

The contents of any sent email must not infringe copyright.

4.0 DATA PROTECTION POLICY

4.1 All employees have a responsibility to observe the statutory requirements of the Data Protection Act 1998, which is now extended to cover not only the collection, storage and use of automatically produced information relating to living individuals, but manual records as well.

4.2 Data subjects (that's the individuals to whom the information relates) have rights of access, and can sue for damages and distress if the information about them is misused or wrongly dealt with. As a consequence, the College and Governing Body (as the responsible authority and employer) could also face legal sanctions by the Data Protection Commissioner resulting in the possible loss of its registration.

4.3 Any questions/queries about the College's obligations with regard to the Data Protection Act 1998 should be referred to the College's Data Protection Officer.

4.4 **Any breach of the Data Protection Policy** will be dealt with in accordance with the College's disciplinary rules and Disciplinary Policy.

DATA PROTECTION POLICY

The *Data Protection Act 1998* contains detailed provisions about the manner in which data is to be collected, stored, accessed and released, but in short the following 8 principles should be observed by all staff:

1. Data must be accurate and where necessary, kept up-to-date.
2. Data must not be held longer than necessary for the purpose for which it is held.
3. Individuals have the right to know if personal data relating to them is held, to see their data and where necessary have it corrected or deleted.
4. Data must be protected against unauthorised access, alteration, destruction and disclosure[#].
5. Data shall be obtained and processed fairly and lawfully.
6. Data shall only be held for specified lawful purposes.
7. Data may not be used or disclosed except for lawful purposes which are described in the register entry[##].
8. Data must be adequate and relevant, but not excessive in relation to the purpose for which it is held.

[#] No logged on desktop/laptop computer should be left unattended at any time.
[#] All confidential electronic data taken off site must be adequately encrypted.

[##] As a general rule of thumb our registration permits disclosure to the *LA*, prospective employers, healthcare, social and welfare advisers/practitioners, local government, police authorities, the courts, *DES*, careers service, *OFSTED* and other regulatory authorities. Transfer of data is confined to the UK/EEC areas only.

5.0 (COLLEGE OWNED) NON-DOMAIN DEVICE ACCEPTABLE USE POLICY

5.1 This policy relates to devices which are owned by the College and that can access the internet either through the school's internet proxy or directly via 3G services. These devices are not part of the College's network domain and so their use is exempt from the **Network Acceptable Use Policy**. Such devices include smartphones and tablets, e.g. Apple iPad.

5.2 The College reserves the right to monitor staff device usage.

5.3 Staff will take responsibility for all activity that takes place whilst using a device.

5.4 Staff may reclaim the cost of any purchase made in regard to a device via a petty cash claim, provided the purchase is in relation to College business. A receipt of purchase will be required and the claim must be countersigned by a budget holder.

5.5 All users should make themselves familiar with the College's **Display Screen Equipment (DSE) Policy** prior to using any device.

5.6 Any user should make themselves familiar with the College's **Data Protection Policy.**

5.7 Any ICT problems/issues should be reported to the IT Department immediately.

5.8 Any breach of the **(College Owned) Non-Domain Device Acceptable Use Policy** will be dealt with in accordance with the College's disciplinary rules and Disciplinary Policy.

(COLLEGE OWNED) NON-DOMAIN DEVICE ACCEPTABLE USE POLICY

Passwords are to be kept confidential.

Individually issued staff devices must not be used by non-College employees.

The use of any device for any illegal purpose is forbidden.

Staff may purchase (using their own funds) and install any application/service, except those that are clearly unsuitable for use in a College or professional environment.

Any account used in the purchase of applications/services for a device must be associated with the College, ie use a College email account as a username/main point of contact.

Unattended devices must be left in a locked room/office. Where security equipment is provided it must be used.

Devices must not be left unattended in a vehicle at any time.