ICT Acceptable Use Policy

The Arts Educational Schools

June 2018

1 **Background**

Overall responsibility: The HR Manager has delegated responsibility for the effective operation of the Staff Handbook including its maintenance and review and for ensuring compliance with employment law.

Changes: From time to time the School may need to make changes to this Policy. This may be in response to periodic review or legislative change. You will be notified in writing of any changes.

Pupil: This refers to any person enrolled at The Arts Educational Schools independent school or sixth form.

Student: This refers to any person enrolled in further education or higher education or ArtsEd Extra at the Arts Educational Schools.

Status: Unless otherwise indicated, the contents of this Policy do not form part of your contract of employment. However, the effect of your contract of employment is that you are under a contractual obligation to provide information as and when requested do so in the policies and procedures such as this one. In some cases, the provision of information may be a statutory requirement as well. A failure to provide certain information may result in the School being unable to meet its employment, safeguarding or legal obligations and may be treated as a disciplinary matter.

Training: Staff will be provided with induction training and ongoing professional development training as appropriate and in accordance with individual development needs.

Queries: If you have any queries about this policy please contact the Finance Director.

Review: This Policy reflects the law and the School's practice as at May 2018. The policies are reviewed annually by the Finance Director.

2 **Introduction**

This policy sets out the requirements with which you must comply when using the School's IT and when otherwise using IT in connection with your job including:

2.1 the School's email and internet services;

2.2 telephones and faxes;

2.3 the use of mobile technology on School premises or otherwise in the course of your employment (including 3G / 4G or Bluetooth or other wireless technologies), whether using a school or a personal device; and

2.4 any hardware (such as laptops, printers or mobile phones) or software provided by, or made available by, the School.

This policy also applies to your use of IT off school premises if the use involves Personal Information of any member of the School community or where the culture or reputation of the School are put at risk.

3 **Failure to comply:** Failure to comply will constitute a disciplinary offence and will be dealt with under the School's disciplinary procedure.

4 **Property:** You should treat any property belonging to the School with respect and reasonable care and report any faults or breakages immediately to the IT Department. You should not

use the School's computers or other IT resources unless you are competent to do so and should ask for training if you need it.

5 **Viruses and other malicious code:** You should be aware of the potential damage that can be caused by computer viruses and other malicious code. You must not use, introduce or operate any hardware, programmes or data (including computer games) or open suspicious emails without permission from the IT Department.

6 **Passwords:** The minimum specification for a password is 8 characters which must contain at least one capital letter, and one number or special character. The password cannot contain your name or part of your name. The minimum password specification is enforced by the network settings managed by the IT Administrator. Your password should not be disclosed to anyone else. In addition:

6.1 your password should be difficult to guess, for example, you could base your password on something memorable that no one else would know. You should not use information which other people might know, or be able to find out, such as your address or your birthday;

6.2 you must not use a password which is used for another account. For example, you must not use your password for your private email address or online services for any school account;

6.3 passwords (and any other security credential you are issued with such as a key fob or USB drive) must be kept secure and confidential and must not be shared with, or given to, anyone else. Passwords should not be written down.

7 **Leaving workstations:** If you leave your workstation for any period of time you should take appropriate action and, in particular, you should lock your screen to prevent access.

8 **Concerns**: You have a duty to report any concerns about the use of IT at the School to the Finance Director. For example, if you have a concern about IT security or pupils and/or students accessing inappropriate material.

9 **Other policies**: This policy should be read alongside the following:

9.1 Staff Code of Conduct;

9.2 internet policy;

9.3 data protection policy for Staff;

9.4 information security policy.

Internet

10 **Downloading:** Downloading of any programme or file which is not specifically related to your job is strictly prohibited.

11 **Personal use:** The School permits the incidental use of the internet so long as it is kept to a minimum and takes place substantially out of normal working hours. Use must not interfere with your work commitments (or those of others). Personal use is a privilege and not a right. If the School discovers that excessive periods of time have been spent on the internet provided by the School or it has been used for inappropriate purposes (as described in section 12 below), either in or outside working hours, disciplinary action may be taken and internet access may be withdrawn without notice at the discretion of the Principal.

12 **Unsuitable material:** Viewing, retrieving or downloading of pornographic, terrorist or extremist material, or any other material which the School believes is unsuitable is strictly prohibited and constitutes gross misconduct. This includes such use at any time on the School's network, or via 3G or 4G when on School premises or otherwise in the course of your employment and whether or not on a School or personal device. Internet access may be withdrawn without notice at the discretion of the Principal whilst allegations of unsuitable use are investigated by the School.

We are obliged to monitor to fulfil our responsibilities with regard to UK law and our duties under the government's Prevent strategy.

13 **Contracts:** You are not permitted to enter into any contract or subscription on the internet (including through an App) on behalf the School, without specific permission from the Finance Director. This applies both to "free" and paid for contracts, subscriptions and Apps.

14 **Retention periods**: the School keeps a record of staff browsing histories for a period of up to six months.

Email

15 **Personal use:** The School permits the incidental use of its email systems to send personal emails as long as such use is kept to a minimum and takes place substantially out of normal working hours. Personal emails should be labelled "personal" in the subject header. Use must not interfere with your work commitments (or those of others). Personal use is a privilege and not a right. The School may monitor your use of the email system, please see paragraphs 23 to 27 below, and staff should advise those they communicate with that such emails may be monitored. If the School discovers that you have breached these requirements, disciplinary action may be taken.

16 **Status:** Email should be treated in the same way as any other form of written communication. Anything that is written in an email is treated in the same way as any form of writing. You should not include anything in an email which is not appropriate to be published generally.

17 **Inappropriate use:** Any email message which is abusive, discriminatory on grounds of sex, marital or civil partnership status, age, race, disability, sexual orientation or religious belief (or otherwise contrary to our equal opportunities policy), or defamatory is not permitted. Use of the email system in this way constitutes gross misconduct. The School will take no responsibility for any offence caused by you as a result of downloading, viewing or forwarding inappropriate emails.

18 **Legal proceedings:** You should be aware that emails are disclosable as evidence in court proceedings and even if they are deleted, a copy may exist on a back-up system or other storage area.

19 **Jokes:** Trivial messages and jokes should not be sent or forwarded to the email system. They could cause the School's IT system to suffer delays and / or damage or could cause offence.

20 **Contracts:** You should not enter into any contractual commitments on behalf of the School with other organisations via email correspondence unless you have the prior authorisation of the Finance Director or Principal.

21 **Disclaimer:** All correspondence by email should contain the School's disclaimer.

22 **Data protection disclosures:** Subject to a number of limited exceptions, potentially all information about an individual may be disclosed should that individual make a subject access request under data protection legislation. There is no exemption for embarrassing information (for example, an exchange of emails containing gossip about the individual will

usually be disclosable). **Staff must be aware that anything they put in an email is potentially disclosable.**

Monitoring

23 The School regularly monitors and accesses its IT system for purposes connected with the operation of the School. The School IT system includes any hardware, software, email account, computer, device or telephone provided by the School or used for School business. Staff should be aware that the School may monitor the contents of a communication (such as the contents of an email).

24 The purposes of such monitoring and accessing include:

24.1 to help the School with its day to day operations. For example, if a member of staff is on holiday or is off sick, their email account may be monitored in case any urgent emails are received; and

24.2 to check staff compliance with the School's policies and procedures and to help the School fulfil its legal obligations. For example, to investigate allegations that a member of staff has been using their email account to send abusive or inappropriate messages.

25 Monitoring may be carried out in response to a specific incident or concern.

26 The School also uses software which automatically monitors internet use (for example, it would raise an alert if a member of Staff attempted to access a blocked website).

27 The monitoring is carried out by the Designated Safeguarding Lead and Facilities Manager. If anything of concern is revealed as a result of such monitoring then this information may be shared with the Finance Director and this may result in disciplinary action. In exceptional circumstances concerns will need to be referred to external agencies such as the Police.

Social media

28 The School recognises that the internet provides unique opportunities to participate in interactive discussions and share information on particular topics using a wide variety of social media, such as Facebook, LinkedIn, Twitter, Instagram, Snapchat and all other internet postings including blogs, wikis and other interactive websites. It is also a valuable educational tool.

29 **Purpose:** This policy applies to the use of social media for School and your own personal purposes, whether during normal working hours or in your personal time. Its purpose is to help staff avoid the potential pitfalls of sharing information on social media sites. This policy is designed for your protection.

30 **IT facilities:** The policy applies regardless of whether the social media is accessed using the School's IT facilities and equipment or your personal devices.

31 **Personal use:** The School permits the incidental use of the internet and social media so long as it is kept to a minimum and takes place substantially out of normal working hours. Use must not interfere with your work commitments (or those of others). Personal use is a privilege and not a right. If the School discovers that excessive periods of time have been spent on the internet provided by the School either in or outside working hours, disciplinary action may be taken and internet access may be withdrawn without notice at the discretion of the Principal.

32 **Guiding principles:** Staff are required to behave responsibly at all times and adhere to the following principles:

SOCIAL MEDIA CONTACT WITH HE STUDENTS

32.1 It is deemed acceptable for staff to connect with current students for professional purposes.

32.2 It is deemed acceptable for staff to connect with past students.

32.3 If you are “Friends” with, “Follow”, have “Followers”, or connect with current or past students on any social media or any other interactive network, you should be mindful of the content and intention of posts, shares, comments or private messages. It is always sensible to consider that any information posted may not remain private.

SOCIAL MEDIA CONTACT WITH DAY SCHOOL AND SIXTH FORM PUPILS

32.4 Staff should not be "Friends" with, "Followers" of, or connect with Day School or 6th form pupils on any social media or other interactive network for any purpose. It would be considered inappropriate to connect with Day School or 6th form pupils on a personal account for any purpose. Depending on the circumstances, it may also be inappropriate to connect with parents, guardians or carers.

GENERAL PRINCIPLES – ALL USE OF SOCIAL MEDIA

32.5 You must not publish anything which could identify students, pupils, parents or guardians on any personal social media account, personal webpage or similar platform without the prior consent of the Principal in writing. This includes photos, videos, or other materials such as pupil and/or student work.

32.6 You must be mindful of how you present yourself and the School on such media. Staff are entitled to a social life like anyone else. However, the extra-curricular life of an employee at the School has professional consequences and this must be considered at all times when sharing personal information.

32.7 You should protect your privacy and that of others by omitting personal information from internet posts such as names, email addresses, home or work addresses, phone numbers or other personal information.

32.8 You should familiarise yourself with the privacy settings of any social media you use and ensure that public access is restricted. If you are not clear about how to restrict access, you should regard all your information as publicly available and behave accordingly.

32.9 You 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.

32.10 You must not post anything that could be interpreted as threatening, intimidating or abusive. Offensive posts or messages may be construed as cyber-bullying.

32.11 You must not post disparaging or derogatory remarks about the School or its Trustees, staff, volunteers, students, pupils, parents, guardians or carers.

32.12 You must not post anything that could be interpreted as glorifying or supporting terrorism, extremism or organisations promoting terrorist or extremist views, or encouraging others to do so.

32.13 You must not use social media in a way which could constitute a breach of any of the School's policies.

33 **Removing postings:** You may be required to remove internet postings which are deemed to constitute a breach of this policy. If you fail to remove postings, this could result in disciplinary action.

34 **Breach:** A breach of this policy may be treated as misconduct and could result in disciplinary action including in serious cases, dismissal.