M1a ICT Acceptable Use Policy (Staff)

Introduction

Information and Communication Technology (ICT) and 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 members of staff are aware of their professional responsibilities when using any form of ICT at school. All members of staff are expected to adhere to the contents of this policy. Any concerns or clarification should be discussed with the IT Manager. For the purposes of this policy, where the phrase "without permission" appears, this means the prior permission of the IT Manager, except where indicated to the contrary.

Scope

This policy applies to all users of ICT facilities which are owned, leased, hired or otherwise provided by the school, ICT facilities connected directly or remotely to the school's IT and ICT facilities used on the school's premises whether or not owned by the school, and used for any purpose whatsoever. It covers personal computers whether desktop, laptop or handheld, computer networks, all software and data thereon and all computer-based information systems, including telephones, provided for administrative or other purposes. Staff using a school laptop or other device off the school site, at home or elsewhere, are therefore required to abide by this policy.

Basic Principles

All users must act responsibly and guard against action that disrupts or threatens the viability of the school's ICT systems, releases confidential data or potentially breaches Child Protection requirements. Every user is responsible for the integrity of the school's systems and must act in accordance with this policy, relevant law and contractual obligations, and apply the highest standard of ethics.

As a member of the school community you should follow these principles in all of your online activities:

- The school cannot guarantee the confidentiality of content created, shared and exchanged via school systems. Ensure that your online communications, and any content you share online, are respectful of others and composed in a way you would wish to stand by.
- Do not access, create or share content that is illegal, deceptive, or likely to offend other members of the school community (for example, content that is obscene, or promotes violence, discrimination, or extremism, or raises safeguarding issues).
- Respect the privacy of others. Do not share photos, videos, contact details, or other information about members of the school community, even if the content is not shared publicly, without going through official channels and obtaining permission.
- Do not access or share material that infringes copyright, and do not claim the work of others as your own.
- Do not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities.
- Staff should not use their personal email, or social media accounts to contact pupils or

parents, and pupils and parents should not attempt to discover or contact the personal email addresses or social media accounts of staff.

Whenever you use the school's IT systems (including by connecting your own device to the network) you should follow these principles:

- Only access school IT systems using your own username and password. Do not share your username or password with anyone else.
- Do not attempt to circumvent the content filters or other security measures installed on the school's IT systems, and do not attempt to access parts of the system that you do not have permission to access.
- Do not attempt to install software on, or otherwise alter, school IT systems.
- Do not use the school's IT systems in a way that breaches the principles of online behavior set out above.
- Remember that the school monitors use of the school's IT systems, and that the school can view content accessed or sent via its systems.

Authority

The designated post-holder with the authority to give access to ICT facilities and to give permissions as stated in this policy is the IT Manager, who is responsible to the Bursar for the provision of all ICT services within the school.

Access Rights and Password Usage

Passwords protect the School's network and computer system and are your responsibility. They should not be obvious (for example "password", 123456, a family name or birthdays), and nor should they be the same as your widely-used personal passwords. You should not let anyone else know your password, nor keep a list of passwords where they may be accessed, and must change it immediately if it appears to be compromised. You should not attempt to gain unauthorised access to anyone else's computer or to confidential information to which you do not have access rights. Staff will be granted the following access rights:

a) Access rights to ICT facilities are provided to all staff who require such access for the proper execution of their jobs.
b) Access to the ICT system, including use of the school's internet and email systems, is not provided as a right to any user and may be withdrawn, in full or in part, from any user as a result of inappropriate use.
c) All users will be provided with a user name and password to enable access to those parts of the IT relevant to their work.
d) Users must not use another user's name or password, nor allow any password issued to them to become known to any other person, nor, having logged in, leave ICT facilities unattended and potentially usable by another person.
e) Once a member of staff has left the school's employment, all their permissions to use ICT facilities cease and their online files will be deleted one month after their employment terminates.

Use of Email

a) Email is the standard form of communication within the school, and all staff are expected to check their emails at least twice a day during term, and always before 08:40 (or at the

start of contact hours in the case of part-time staff). If you are going to be out of School please use the "out of office" facility.

b) E-mails from parents should be acknowledged as soon as possible, and always within one working day. If the matter requires investigation or discussion with other staff, you should explain this to the parent and give some indication of when they may expect a fuller reply.
c) Treat confidential material in the same way as you would if you were sending a hard copy: consider the consequences if a third party were to read what you have written. If you write about a student, write as if he/she has access to the email. In law, they do, and the school may have to disclose e-mails if a formal request is made. Remember that e-mails can be sent to anyone instantly – confidentiality cannot be assumed.
d) If sending a reply or forwarding an e-mail from someone else, remember that it will usually include the history or "thread" of earlier messages. You may not want to send this (especially to external recipients) unless it is relevant
e) Any email sent from a school email account has the same status as a letter written on the school's headed paper: it is an official communication which carries an implicit endorsement from the school. No email may therefore be sent which might in any way bring discredit or embarrassment to the school, or bring the school into disrepute.
f) Likewise staff should only use the approved, secure email system for any school business and under no circumstances should staff contact students, parents or conduct any school business using their personal e-mail.
g) Users who receive any email which they regard as illegal, inappropriate or offensive should report it immediately to their line manager, or the Bursar.
h) Where confidential information needs to be sent by e-mail the document must be encrypted, using the encryption functionality within windows applications. Where this is not possible users should liaise with the IT Manager to find an appropriate solution.
i) Never send multi-destination e-mails in which another colleague is criticised, implicitly or explicitly. Avoid criticising named students in a personal way – think how the parents might react if the e-mail should find its way to them. If you need to write about students, stick to the facts in disciplinary and academic matters without expressing unduly critical opinions of your own.
j) Only copy in colleagues if absolutely necessary. If you wish to send to a large group – perhaps all staff or the visiting instrumental staff there are pre-set groups set up in the main directory.

Use of the Internet

a) Staff may access the internet only for purposes associated with their role within the school (except as permitted under 10. below).
b) Staff may not, under any circumstances, download, store, create, display, print, produce, circulate or transmit offensive and/or harassing material in any form or medium, or material which is designed or likely to cause annoyance, inconvenience or distress, or that is liable to damage the reputation of the school.
c) There are filtering controls on the internet to prevent access to unsuitable material and the controls in place take account of the School's responsibilities under the Prevent Duty guidance.
d) Staff who inadvertently access any unacceptable site or material as a result of an innocent internet query must report it immediately to IT Support.

Security

The school has in place an extensive and effective Firewall, which should prevent the downloading of inappropriate material, and a comprehensive anti-virus system. However, no system is 100% effective, and all staff have a responsibility to help to protect the school from computer virus attack or technical disruption. In particular, users must not:

- Download/run any applications (apps), programs, or other executable files without permission.
- Open an attached program file with a file extension of ".exe", ".com", ".scr" or ".bat", or any attachment that look in any way suspicious unless absolutely certain that it has come from a trusted source.

If in doubt, consult the IT Manager before opening any email, attachment or other file.

Data Protection

a) All users are required to comply with the Data Protection Act 1998. This requires the school and all employees of the school to ensure that personal data held about individuals (staff, parents and students) is not passed to those who do not need to know for the purposes of their role at the school. In particular, data such as home addresses and telephone numbers, medical history, family information, access to counselling or other services, and photographs of students must not be disclosed without good reason. If in doubt the School's Data Protection policy should be consulted.
b) Staff should be particularly aware of the potential for inadvertent disclosure through the use of SIMS on an interactive whiteboard, and through the use of laptops in public places.
c) Staff with access to SIMS should ensure that computers are not left logged on in unlocked offices or classrooms where they can be accessed by unauthorised personnel.

Personal Use

All official school business of staff must be conducted on school systems, and it is not permissible to use personal email accounts for school business. Any use of personal devices for school purposes, and any removal of personal data or confidential information from school systems – by any means including email, printing, file transfer, cloud or (encrypted) memory stick – must be registered and approved by IT department.

a) Personal use of the school's ICT facilities (including the email system and internet) is permitted, provided that it is reasonable, does not breach this policy, does not involve excessive cost to the school, does not impinge on other users, and is not for commercial gain. In particular, use of school printers for multiple copies, or any use of colour printers, should be restricted to school business only, except by arrangement with the Deputy Bursar, who will charge for any such use at cost.
b) Staff may use social networking sites, but should be aware that usage may be monitored, and any excessive or inappropriate use will be addressed. The school reserves the right to withdraw access to social networking sites or personal blogs at any time.
c) It is therefore critical to the safety and security of the school IT that the following points are adhered to;
    i. It is the responsibility of device owners/users to ensure that their equipment is correctly configured and maintained; that it has current Operating System updates

and other security patches applied, and is running effective firewall and virus protection software at all times.

ii. The school can take no responsibility for loss/damage of any personal software/data/hardware, whatever the cause.

iii. Staff may not plug any device into the Ethernet/physically-cabled part of the school IT.

iv. Wireless connection must only be made through the official Purcell School wireless IT. Access will only be allowed using your Purcell School user name and password.

Monitoring

Staff, parents and pupils should be aware that school email and internet usage (including through school Wi-Fi) will be monitored for safeguarding, conduct and performance purposes, and both web history and school email accounts may be accessed by the school where necessary for a lawful purpose – including serious conduct or welfare concerns, extremism and the protection of others. Any personal devices used by pupils, whether or not such devices are permitted, may be confiscated and examined under such circumstances. The school may require staff to conduct searches of their personal accounts or devices if they were used for school business in contravention of this policy, and in particular if there is any reason to suspect illegal activity or any risk to the wellbeing of any person.

a) The school reserves the right to monitor use of its ICT facilities at any time without notice to ensure they are not being misused or this policy breached.
b) The IT Manager may, during routine maintenance, access staff file areas to ensure the safe and smooth running of the IT.
c) The IT Manager may also require users to return laptops or other school equipment on demand and without notice for routine maintenance.
d) In order to protect the IT and users, access to some websites may from time to time be blocked. Staff who require access to any blocked site should contact the IT Manager.

Equipment

a) Users are responsible for ensuring that they are sufficiently familiar with the operation of any equipment they use to make their use of it safe and effective, and to avoid interference with the use of it by others.
b) Users must take every precaution to avoid damage to equipment. To save electricity and extend the life of the equipment, all computers, data projectors and other devices should be switched off at the end of each working day.
c) Digital cameras, mp3 players and USB data storage devices must be connected only through USB ports provided for that purpose. No other equipment may be connected in any way into any IT, workstation, or other ICT facility without permission from the IT Manager.
d) No equipment (other than laptops issued to staff) or other ICT facility may be physically moved or borrowed without permission.

Arrangements for Students e-safety

The ICT Acceptable Use Policy for Students covers the key systems and controls in place. These include;

a) Password controls and access control by year and age.

b) E-safety training is provided for students through the PSHE programme, specific assemblies, House-meetings and tutorials.
c) Robust filtering arrangements which are reviewed regularly. Details of the filtering matrix are available from the IT Manager.

Arrangements for Visitors

Where visitors need access to the wireless IT, guest access can be arranged. The person hosting the visit should contact the IT Manager in good time. He will provide a user account, details of how to access the user account and the Purcell School's acceptable use policy as it relates to visitors. Staff members hosting visitors are responsible for supervising their visitors and ensuring that all School procedures are followed.

Personal Social Media Accounts

All adults working in a school environment should be aware of the many challenges and ramifications associated with the use of electronic communication and social media.

Whilst the School recognises the individual's right to a private life, staff using Social Media sites or maintaining personal blogs must refrain from making any reference to the school, staff or students that could bring the School into disrepute and only use information that is already published by the School.

Sound judgement and due care should be exercised in using social media as conduct by staff which may not directly relate to students may be relevant to their (real or perceived) suitability to have contact with children. Unwise behaviour online can result in criminal action, being placed on List 99 (unsuitable to work with children) and even being placed on the Sex Offenders' Register.

In particular all staff must:

a) only use official channels of communication (e.g. work e-mail addresses) and be aware of and comply with the school's policies and guidance;
b) never exchange private text, phone numbers, personal e-mail addresses or photos of a personal nature with students;
c) firmly decline student-initiated 'friend' or equivalent requests from students or where necessary block the request and do not instigate any yourself. Use your own discretion when dealing with 'friend' or equivalent requests from parents. It is acceptable to decline these invitations and remind parents of more formal channels which they can discuss their child's education;
d) we advise that you do not initiate any friend or equivalent requests with ex-students.
e) operate online in a way in which would not call into question your position as a professional;
f) realise that students will be naturally curious about staff member's personal lives outside school and may try to find additional information on-line.
g) manage your privacy setting and keep them under regular review. These are particularly important in regard to photos, and remember that no privacy mechanism is 100% guaranteed;
h) ensure settings prohibit others from tagging you in any photos or updates without your permission and that you can ask others to remove any undesirable content related to you;
i) audit and re-evaluate the online information about you and who has access to it;
j) where a teacher has a professional role outside school and as part of that role needs to

highlight the work that they do this should be done via a professional pages and permission obtained in writing from the Principal where the Purcell School will be named;

k) assume that information you post can be accessed and altered;
l) not discuss students, colleagues, parents online or criticise their employer or others within the school community;
m) not post pictures of Purcell School students
n) respect student privacy and confidentiality at all times;
o) use strong passwords and change them regularly. Protect mobile phone/smart phone/tablet computer with a PIN, especially when in school to protect access to content and potential misuse.
p) seek approval from the Head before you speak about or make any comments on behalf of the school on the internet or through any social ITing site;
q) weigh whether a particular posting puts your effectiveness as a member of staff at The Purcell School at risk;
r) post only what you want the world to see.

If you are the victim of cyber-bullying or are uncomfortable with comments, photos or posts made online of or about you or others, please bring the matter to the attention of the Deputy Head (Staff) or the Bursar immediately.

Official School Social Media Accounts

The School currently has the following official social media accounts: Facebook, Twitter, and Instagram. These are overseen by the PR and Communications Manager. The Concerts and Events Manager and Concerts Assistant also have access. Staff wishing to promote events or activities should contact the Concerts and Events Manager (for Concerts) and the Publicity and Communications Manager (for other events) a minimum of one week before the event.

Breach Reporting

The law requires the school to notify personal data breaches, if they are likely to cause harm, to the authorities and, in some cases, to those affected. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This will include almost any loss of, or compromise to, personal data held by the school regardless of whether the personal data falls into a third party's hands. This would include:

- loss of an unencrypted laptop, USB stick or a physical file containing personal data;
- any external hacking of the school's systems, eg through the use of malware;
- application of the wrong privacy settings to online systems;
- misdirected post, fax or email;
- failing to bcc recipients of a mass email; and
- unsecure disposal.

The school must report personal data breaches to the ICO without undue delay (ie within 72 hours), and certainly if it presents a risk to individuals. In addition, controllers must notify individuals affected if that risk is high. In any event, the school must keep a record of any personal data breaches, regardless of whether we need to notify the ICO.

If either staff or pupils become aware of a suspected breach, the school must take steps to ensure

they are as rare and limited as possible and that, when they do happen, the worst effects are contained and mitigated. This requires the involvement and support of all staff and pupils. The school's primary interest and responsibility is in protecting potential victims and having visibility of how effective its policies and training are. Accordingly, falling victim to a data breach, either by human error or malicious attack, will not always be the result of a serious conduct issue or breach of policy; but failure to report a breach will be a disciplinary offence.

Breaches of this Policy

A deliberate breach of this policy by staff will be dealt with as a disciplinary matter using the school's usual applicable procedures. In addition, a deliberate breach by any person may result in the school restricting that person's access to school IT systems.

If you become aware of a breach of this policy or the e-Safety Policy, or you are concerned that a member of the school community is being harassed or harmed online you should report it to Adam Wroblewski, Bursar. Reports will be treated in confidence wherever possible.

Acceptance of this Policy

Please confirm that you understand and accept this policy by signing below and returning the signed copy to Simon Kingsbury, IT Network Manager

I understand and accept this acceptable use policy:

Signed ……..

Policy author/reviewer:	*Policy date/review date:*	*Next review date:*
Paul Bambrough	January 2020	January 2021
Adam Wroblewski	September 2021	September 2022