

ARCHBISHOP TEMPLE SCHOOL



Staff & Volunteer ICT Acceptable Use Policy & Guidance

**(incorporating Email Use Policy;
Social Networking Sites &
Social Media Policy)**

Date Agreed : November 2018

To Be Reviewed : November 2019

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communication technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for pupils' learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, iPads, email, VLE etc) out of school.
- I understand that the school ICT systems (including desktops, laptops and iPads) are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school. I agree not to use the school's ICT system and resources for personal use when I am supervising pupils or teaching classes.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies. I have been advised about good practice in the use of chat and social networks in my personal time and I acknowledge that I will not receive any support from the school for any consequences of failing to follow these guidelines.
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner. I will not use personal email addresses to communicate with pupils, parents or former pupils under the age of 18. I will not reply to emails from pupils that do not use the pupil's school email address.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held / external devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies or approved by the school's network manager.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others. I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy. Where personal data is transferred outside the secure school network, it must be encrypted.

- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

Email Use Policy

All users

- School email accounts should be the only account that is used for school-related business.
- The school reserves the right to block external personal email accounts.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged. A full audit trail can be made available should this become necessary.
- Pupils and staff should be aware of the dangers of opening email from an unknown sender or source or viewing and opening attachments.
- All email users within school should report any inappropriate or offensive emails through the incident-reporting mechanism within school.
- Irrespective of how pupils or staff access their school email (from home or within school), school policies still apply.

Staff

- Staff should not use personal email accounts for professional purposes, especially to exchange any school-related information or documents.
- Staff will only use official school-provided email accounts to communicate with pupils and parents and carers.
- Emails containing personal, confidential, classified or financially sensitive data to external third parties or agencies needs to be controlled and never communicated through the use of a personal account.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- Staff should discourage the pupils' use of personal emails, and never reply to an email from a pupil using their own personal email account.
- Excessive social email use can interfere with learning and productivity and staff are asked to restrict this in line with the school Safeguarding, Online Safety and Acceptable Use Policies.
- The school requires a standard disclaimer to be attached to all email correspondence except those of the Headteacher, stating that, 'the views expressed are not necessarily those of the school'.
- Email accounts should be checked regularly for new correspondence.
- When away for extended periods, 'out-of-office' notification should be activated so that colleagues are aware that you are not currently available.

Pupils

- Pupils will be allocated an individual email account for their own use in school or class. This account has a password which pupils must keep secure.
- Pupils may only use school-approved accounts on the school system.
- Pupils should be reminded frequently about the dangers of revealing personal information within email conversations.
- Pupils should be reminded frequently not to reveal personal details of themselves or others in email communications. Pupils should get prior permission from an adult if they arrange to meet with anyone through an email conversation.
- All pupils with active email accounts are expected to adhere to the generally accepted rules of etiquette; particularly in relation to the use of appropriate language. They should not reveal any personal details about themselves or others in email communication or arrange to meet anyone without specific permission.
- Any inappropriate use of the school email system or receipt of any inappropriate messages from another user should be reported to a member of staff immediately.
- Pupils must immediately tell a teacher or trusted adult if they receive any inappropriate or offensive email.

Policy on the Use of Social Networking Sites and Other Forms of Social Media

1. Introduction

This Policy sets out the school's position regarding the use of social networking sites and other forms of social media. The aim of the document is to ensure that all employees are fully aware of the risks associated with using such sites and their responsibilities with regards to the safeguarding and protection of both children and themselves.

This policy has been developed in consultation with the recognised Trade Unions and professional Associations.

2. Background

2.1 The use of social networking sites such as Facebook, Bebo, Twitter and MySpace has over recent years become the primary form of communication between friends and family. In addition there are many other sites which allow people to publish their own pictures, text and videos such as YouTube and Instagram.

2.2 It would not be reasonable to expect or instruct employees not to use these sites which, if used with caution, should have no impact whatsoever on their role in school. Indeed, appropriate use of some sites may also have professional benefits. For example many schools now use sites such as Facebook and Twitter as a means to enhance parental engagement.

2.3 It is now widely acknowledged that use of such sites does not provide a completely private platform for personal communications. Even when utilised sensibly and with caution employees are vulnerable to their personal details being exposed to a wider audience than they might otherwise have intended. One example of this is when photographs and comments are published by others without the employees consent or knowledge which may portray the employee in a manner which is not conducive to their role in school.

2.4 Difficulties arise when staff utilise these sites and they do not have the relevant knowledge or skills to ensure adequate security and privacy settings. In addition there are some cases when employees deliberately use these sites to communicate with and/or form inappropriate relationships with children and young people.

3. Guidance And Advice

3.1 Employees who choose to make use of social networking site/media should be advised as follows:-

- (i) That they should not access these sites for personal use during working hours;
- (ii) That they familiarise themselves with the site's 'privacy settings' in order to ensure that information is not automatically shared with a wider audience than intended;
- (iii) That they do not conduct or portray themselves in a manner which may:-
 - bring the school into disrepute;
 - lead to valid parental complaints;
 - be deemed as derogatory towards the school and/or it's employees;
 - be deemed as derogatory towards pupils and/or parents and carers;
 - bring into question their appropriateness to work with children and young people.

- (iv) That they do not form on-line 'friendships' or enter into communication with *parents/carers and pupils as this could lead to professional relationships being compromised.
- (v) On-line friendships and communication with former pupils should be strongly discouraged particularly if the pupils are under the age of 18 years.

*(*In some cases employees in schools/services are related to parents/carers and/or pupils or may have formed on-line friendships with them prior to them becoming parents/carers and/or pupils of the school/service. In these cases employees should be advised that the nature of such relationships has changed and that they need to be aware of the risks of continuing with this method of contact. They should be advised that such contact is contradictory to this Policy and as such they are potentially placing themselves at risk of formal action being taken under the school's Disciplinary Procedure.)*

3.2 Schools should not access social networking sites in order to 'vet' prospective employees. Such practice could potentially create an un-level playing field and lead to claims of discrimination if for example the selection panel were to discover a candidate held a protective characteristic as defined by the Equality Act.

4. Safeguarding Issues

Communicating with both current and former pupils via social networking sites or via other non-school related mechanisms such as personal e-mails and text messaging can lead to employees being vulnerable to serious allegations concerning the safeguarding of children and young people.

The Department for Education document 'Guidance for Safer Working Practices for Adults Working with Children and Young people in Educational Settings (March 2009) states:-

<p>12. Communication with Pupils (<i>including the Use of Technology</i>)</p> <p>In order to make best use of the many educational and social benefits of new technologies, pupils need opportunities to use and explore the digital world, using multiple devices from multiple locations. It is now recognised that that e.safety risks are posed more by behaviours and values than the technology itself. Adults working in this area must therefore ensure that they establish safe and responsible online behaviours. This means working to local and national guidelines on acceptable user policies. These detail the way in which new and emerging technologies may and may not be used and identify the sanctions for misuse. Learning Platforms are now widely established and clear agreement by all parties about acceptable and responsible use is essential.</p>	<p><i>This means that schools/services should:</i></p> <ul style="list-style-type: none"> - have in place an Acceptable Use policy (AUP); - continually self-review e-safety policies in the light of new and emerging technologies; - have a communication policy which specifies acceptable and permissible modes of communication.
--	--

<p>Communication between pupils and adults, by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones text messaging, e-mails, digital cameras, videos, web-cams, websites and blogs. Adults should not share any personal information with a child or young person. They should not request, or respond to, any personal information from the child/young person, other than that which might be appropriate as part of their professional role. Adults should ensure that all communications are transparent and open to scrutiny.</p> <p>Adults should also be circumspect in their communications with children so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as grooming. They should not give their personal contact details to pupils including e-mail, home or mobile telephone numbers, unless the need to do so is agreed with senior management and parents/carers. E-mail or text communications between an adult and a child young person outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications through internet based web sites.</p> <p>Internal e-mail systems should only be used in accordance with the school/service's policy.</p> <p>Further information can be obtained from http://www.education.gov.uk/</p>	<p><i>This means that adults should:</i></p> <ul style="list-style-type: none"> - ensure that personal social networking sites are set at private and pupils are never listed as approved contacts; - never use or access social networking sites of pupils; - not give their personal contact details to pupils, including their mobile telephone number; - only use equipment e.g. mobile phones, provided by school/service to communicate with children, making sure that parents have given permission for this form of communication to be used; - only make contact with children for professional reasons and in accordance with any school/service policy; - recognise that text messaging should only be used as part of an agreed protocol and when other forms of communication are not possible not use internet or web-based communication channels to send personal messages to a child/young person.
---	--

5. Recommendations

- (i) That this policy document is shared with all staff who come into contact with children and young people, that it is retained in Staff Handbooks and that it is specifically referred to when inducting new members of staff into your school/service.
- (ii) That appropriate links are made to this document with your school/services Acceptable Use Policy
- (iii) That employees are encouraged to consider any guidance issued by their professional association/trade union concerning the use of social networking sites
- (iv) That employees are informed that disciplinary action may be taken in relation to those members of staff who choose not to follow the advice and guidance outlined in this Policy.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name

Signed

Date