Archbishop Temple School

A Church of England Specialist College

Staff & Volunteer ICT Acceptable Use

Policy & Guidance

Date Agreed : November 2020

To Be Reviewed : November 2021

Name of Policy: **Staff & Volunteer ICT Acceptable Use Policy & Guidance**

Sub-Committee Responsible: **Personnel Committee**

Lead Responsibility in School: **Assistant Headteacher**

Source of Policy: (Please tick)

- **LA:**
- **Diocesan:**
- **School: X**
- **Other – Please specify:**

This policy supports our work as a Church school as summarised in our Vision Statement:

Purpose
Archbishop Temple School seeks to care for young people and prepare them well for adulthood, valuing the whole person.

Mission
Through our faith in God, Father, Son and Holy Spirit, we strive to nurture each person's ability, gifts and talents so that they can 'have life and have it to the full' (John 10:10) and use it in the service of God and other people.

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 support the implementation of the Department for Education's Keeping Children safe in Education September 2020

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 will not use my mobile phone on site in the presence of pupils.
- 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 use chat and social networking sites in accordance with the school's policies and adhering to the social media guidance. 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 secure my personal usb devices that I use in school by password encryption.
- All my documents containing any sensitive data, especially that pertaining to pupils, will be password protected and only shared as an email attachment. I will send the password on a separate email.
- I will not share sensitive data via One Drive.
- I will share only teaching and learning resources on One Drive.
- 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 report any suspicious emails to the IT Network Manager and not open them before checks have been carried out.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not 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 will not connect any of my personal mobile devices to the school wireless network.

- 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.

- To ensure good classroom management, I will monitor the pupils' use of iPads through Apple Classroom when iPads are used in lessons.

- I will adhere to the Acceptable Use Policy for Live Lessons, when teaching through a digital platform.

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

See also Archbishop Temple School's Email Communications 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 use only 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.
- Email attachments containing personal, confidential, classified or financially sensitive data sent to external third parties or agencies must be password protected. The password must be sent on a separate email.
- 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.

Acceptable Use Policy for Live Lessons

See also Archbishop Temple School's Remote Learning Policy

The Department for Education's guidance for Safeguarding and Remote Education During Coronavirus

Teachers

1. Teachers will host live lessons using Teams where and when they find this will enhance the learning experience for the students and where this medium is the most effective to facilitate learning to fulfil the school's legal duty to provide remote education for children unable to attend school due to coronavirus (Covid-19) .
2. Teachers will book live lessons using the calendar in Teams as soon as they are able to respond to information provided regarding the identity of pupils self-isolating and/or working remotely.
3. Teachers will be dressed appropriately and remain professional throughout the video.
4. Teachers will ensure no other family members are in view of the camera.
5. When conducting a live lesson from the teacher's home, teachers will ensure they conduct all videoing with a plain background. If this is not possible then video must be turned off. Use of virtual backgrounds may only be used if there is a plain wall behind to avoid any unfortunate intrusion of the teacher's home i.e. hacking or equipment failure.
6. Teachers must ensure that the option to block incoming video has been selected prior to pupils joining the live lesson
7. Teachers will not conduct live lessons with students outside the hours of 8.40am to 2.45pm.

8. All videos will be recorded for safeguarding purposes. These are stored automatically on the school's Streams account.
9. Live lesson recording must not be downloaded to personal equipment.
10. No video lessons will be one-to-one. If only one student turns up for the meeting and no one else arrives, end the video. A ratio of 1:5 (teacher:student) is required for the lesson to take place, pupils should accept the live lesson invite prior to the lesson commencing.

Students

1. Teachers will only conduct live lessons with students within the hours of 8.40am to 2.45pm.
2. Pupils must not attempt to switch on their web cam/cameras.
3. Pupils must remain on mute until invited to speak.
4. Pupils should be ready and waiting at the starting time of the lesson – this means the student has looked at the Firefly task in advance, appropriate books and writing equipment are ready and devices are prepared to receive the call via Teams.
5. Pupils are prohibited from recording or capturing/screen grabbing content from the video call.
6. Pupils should remain in a public part of their house wherever possible.
7. Devices should not be used in the bathroom or anywhere in the house your parents do not give permission.
8. Pupils may have their school Microsoft Accounts temporarily suspended if they behave inappropriately.
9. Pupils must accept the live lesson Teams invite prior to the lesson beginning.

Parents

1. Parents/carers should ensure their child is appropriately dressed for sessions.
2. Parents/carers should ensure that their child is aware of the need to behave in a session delivered by video link in the same way as if they were in school with the member of staff. If a student is behaving inappropriately, we may suspend their school Microsoft account temporarily.
3. Parents/carers should ensure other household members do not contribute to the live lesson.
4. Parents/carers should ensure their child understands the expectations of how the live lesson will be conducted.
5. Make sure that your child knows their login details and has all relevant equipment set up, so that they are ready to go at the appointed time.

Guidance and support for Parents and Carers

Please let them have some privacy. They need to be able to participate without worrying about you overhearing them, so let them set up in a location that gives them some latitude.

Plug in and close all other tabs: Video-conferencing uses a lot of machine power. It's a good idea to keep devices plugged into the mains power.

Don't take devices into the bathroom: just as with regular school, students should go to the bathroom before class. If there's an emergency, ensure that the microphone is muted.

Be respectful of others: as in the classroom we expect our students to be courteous to the teacher and to others. Impress upon them the fact that this is an unusual time for everyone, and appropriate behaviour should be maintained at all times.

Live lessons will be recorded by the teacher delivering the lesson and these recordings will be stored on Streams.

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 including but not limited to WhatsApp, Facebook, Instagram, Twitter, TikTok and Snapchat 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, TikTok and Instagram.

2.2 It would not be reasonable to expect or instruct employees not to use these sites which, if used without bringing the school or the individual into disrepute, 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 site for personal use whilst in the presence of pupils;

(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 Employees who choose to make use of social networking site/media as part of departmental work or school trip should be advised as follows: -

(i) They should only undertake this role when the Head of Department/Faculty or trip leader has nominated them to do so;

(ii) They should only use nominated social media site/media nominated by the Head of Department/Faculty or trip leader;

(iii) The nominated social media site/media should be set up using an ATS email address only and not a personal email address such as gmail;

(iv) 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;

(v) That they have shared the social media site/media handle with L.Brown (insert Lisa's formal role here) to ensure curation of all posts made;

(vi) Where photographs of pupils are used;
   a. Parental/career permission has been obtained in advance
   b. Checks have been made with L.Brown (insert Lisa's formal role here) to ensure no child's photograph is used when it should not for example, in the case of LAC
   c. The child's name is not posted with the photograph

(vii) That they conduct themselves in a manner that will not bring themselves or the school into disrepute (please also see 3.1(iii-v);

(viii) They should ensure that the account access email has been changed to the next nominated departmental colleague upon leaving the school, where is isn't possible deleting the account.

3.3 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 Practice for Adults who work with Children and Young People in Education (2019) and Addendum April 2020 states:-

12. Communication with Pupils *(including the Use of Technology)*	
In order to make best use of the many educational and social benefits of new and emerging technologies, pupils need opportunities to use and explore the digital world. Online risks are posed more by behaviours and values than the technology itself. Staff should ensure that they establish safe and responsible online behaviours, working to local and national guidelines and acceptable use policies, which detail how new and emerging technologies may be used. Communication with children both in the 'real' world and through web based and telecommunication interactions should take place within explicit professional boundaries. This includes the use of computers, tablets, phones, texts, e-mails, instant messages, social media such as Facebook and Twitter, chat-rooms, forums, blogs, websites, gaming sites, digital cameras, videos, web-cams and other hand-held devices. (Given the ever-changing world of technology it should be noted that this list gives examples only and is not exhaustive.) Staff should not request or respond to any personal information from children other than which may be necessary in their professional role. They should ensure that their communications are open and transparent and avoid any communication which could be interpreted as 'grooming behaviour'. Staff should not give their personal contact details to children for example, e-mail address, home or mobile telephone numbers, details of web-based identities. If children locate these by any other means and attempt to contact or correspond with the staff member, the adult should not respond and must report the matter to their manager. The child should be firmly and politely informed that this is not acceptable.	This means that adults should: ▪ not seek to communicate/make contact or respond to contact with pupils outside of the purposes of their work ▪ not give out their personal details ▪ use only the equipment and internet services provided by the school or setting, unless school policies state otherwise ▪ only use internet-enabled personal devices in line with school acceptable use policies ▪ follow their school / setting's acceptable use policy and online safety guidance ▪ ensure that their use of technologies could not bring their employer into disrepute ▪ not discuss or share data relating to children/ parents / carers in staff social media groups

When selecting a platform for online / virtual teaching, settings should satisfy themselves that the provider has an appropriate level of security. Wherever possible, staff should use school devices and contact pupils only via the pupil school email address / log in. This ensures that the setting's filtering and monitoring software is enabled. In deciding whether to provide virtual or online learning for pupils, senior leaders should take into account issues such as accessibility within the family home, the mental health and wellbeing of children, including screen time, the potential for inappropriate behaviour by staff or pupils, staff access to the technology required, etc. Virtual lessons should be timetabled and senior staff, DSL and / or heads of department should be able to drop in to any virtual lesson at any time – the online version of entering a classroom. Staff engaging in online learning should display the same standards of dress and conduct that they would in the real world; they should also role model this to pupils and parents. The following points should be considered:- ▪ think about the background; photos, artwork, identifying features, mirrors – ideally the backing should be blurred ▪ staff and pupils should be in living / communal areas – no bedrooms ▪ staff and pupils should be fully dressed ▪ filters at a child's home may be set at a threshold which is different to the school ▪ resources / videos must be age appropriate – the child may not have support immediately to hand at home if they feel distressed or anxious about content It is the responsibility of the staff member to act as a moderator; raise any issues of suitability (of dress, setting, behaviour) with the child and / or parent immediately and end the online interaction if necessary Recording lessons does not prevent abuse. If staff wish to record the lesson they are teaching, consideration should be given to data protection issues; e.g., whether parental / pupil consent is needed and retention / storage. If a staff member believes that a child or parent is recording the interaction, the lesson should be brought to an end or that child should be logged out immediately. Staff, parent and pupil AUPs should clearly state the standards of conduct required. If staff need to contact a pupil or parent by phone and do not have access to a work phone, they should discuss this with a senior member of staff and, if there is no alternative, always use 'caller withheld' to ensure the pupil / parent is not able to identify the staff member's personal contact details.	This means that education settings should: • wherever possible, provide school devices such as cameras and mobile phones rather than expecting staff to use their own (e.g. on school trips)

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	