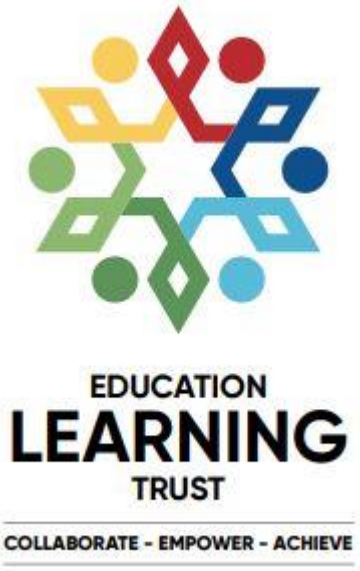

ICT Acceptable Use Policy 2022

Signed by:	Signed by:
Michelle Murray, Executive Principal / CEO	Helen White, Chair of Trustees
Date: 16/03/2022	Date: 16/03/2022

Revision History

Date	Document Version	Document Revision History	Document Author / Reviser	Document Approver
September 2019	1.0	Draft Policy. Reformatted and no significant changes.	ELT J Jones, SBM	Ratified on 25/09/2019 by Trust Board then circulated to Academies
January 2019	1.1	Amended for GDPR purposes re staff & governor emails and children's watches with phone capability.	J Jones ELT Primary SBM	Ratified on 05/02/2020 by Trust Board then circulated to Academies.
September 2020	1.2	Annual document review. No significant changes.	J Jones ELT Primary SBM	Approved on 11/10/20 following Trust Board meeting on 23/09/20, circulated to Admin Managers/Headteachers on 11/10/20 to circulate to staff and AGBs.
January 2021	1.3	Amended to clarify use of governor emails only for school related communications. Pgs. 3,6 & 13.	J Jones ELT HR and Compliance Manager	Approved at Trust Board 24/02/2021. Circulated to academies for staff 05/03/2021
March 2022	1.4	Review of policy to update and ensure fir for purpose for all schools in the Trust (primary and secondary) Circulated to schools on 21/03/2022	R Harte, Network Manager, Werneth School and M Humphreys, Network Manager, The Kingsway School	Trust Board 16/03/2022

Contents

1. Introduction

This acceptable use policy is designed to outline staff responsibilities when using technology, whether this is via personal devices or school devices, or on/off the school premises, and applies to all staff, volunteers, contractors and visitors.

The Education Learning Trust understands that information and communication technology plays an imperative role in the learning, operation, support and governance of the school. All children, staff, governors and volunteers working in or on behalf of the school must use technology appropriately, safely and legally.

We have a responsibility to make all individuals aware of the appropriate behaviour and critical thinking skills to enable them to remain both safe and legal when using the internet and digital technologies in all of its forms. This policy is linked, and works alongside the school's Computing, Safeguarding, E-Safety, Mobile Phone Policy, Data Protection and Record Management policies and Privacy Notices.

2. Privacy

The GDPR and Data Protection Act 2018 require all personal and special category data to be processed with the utmost credibility, integrity and accuracy. This applies to all data the school stores on its network regarding staff, children and other natural persons it deals with whilst carrying out its functions.

The school will only process data in line with its lawful basis to uphold the rights of both children's and staff and other third parties.

In order to protect children's safety and wellbeing, and to protect the school from any third party claims or legal action against it, the school may view any data, information or material on the school's ICT systems (whether contained in an email, on the network, in the cloud or any physical device) and in certain circumstances, disclose that data, information or material to third parties, such as the police or social services. The school Privacy Notices detail the lawful basis under which the school is lawfully allowed to do so.

The school disclaimer that automatically appears at the end of each of your emails notifies the recipient that any email correspondence between you may be monitored. You must not remove this disclaimer. You should bring to the attention of any person who wishes or intends to send you an email that the school may monitor the content of their email.

3. Responsibility for E-Safety and Appropriate Use of ICT

- The Education Learning Trust has responsibility for ensuring that the schools have an Acceptable Use Policy for ICT and this policy is reviewed annually.
- The Head of School will ensure that the Senior Leadership Team takes responsibility for and coordinates e-Safety and acceptable use of ICT within the school. This activity will be closely aligned to the activities of safeguarding and promoting the welfare of all children within the school (see Safeguarding Policy).
- All staff have a responsibility to use ICT appropriately and legally and report any illegal or inappropriate use of ICT to the Head of School or the designated person for e-Safety, as soon as possible.
- All Staff should address issues of e-Safety when using the internet with children.
- Elected governors and volunteers have a responsibility to use school based ICT devices appropriately. Where school information is being communicated between the school and governors, this will be done via a school or the Trust (for Trustees and Members) issued email address and / or via access to a password protected area of the school website or

network only. Email addresses used for the purpose of communications via the Governor Hub must also be the school/Trust issued email to safeguard the information held on and communicated to and from the Governor Hub.

- All children, staff, governors and volunteers must follow all the Acceptable Usage Agreement (see Appendix 1).
- The ICT technical support team responsible for the school will ensure that computers have up to date virus protection and internet connection is appropriately filtered.

4. Use of the Internet

The school ensures that users make effective use of the internet. Use of the internet should always be lawful and appropriate. Internet usage means any connection to the internet via web browsing, external email, social media or news groups.

This policy and code of practice is designed to reduce and control the risk of offences being committed, liabilities being incurred, staff or other children being offended and the school's facilities and information being damaged.

Staff must not give any personally identifiable information concerning the school, its children or parents, or any other member of staff when accessing any website or service. This prohibition covers the giving of names of any of these people – the only exception being the use of the school's name and your name when accessing a service which the school subscribes to.

Staff must not make any changes to any of the school's hardware or software. This prohibition also covers changes to any of the browser settings.

The settings put in place by the school are an important part of the school security arrangements and making any changes, however innocuous they might seem, could allow hackers and computer viruses to access or damage the school's systems.

Staff should assume that all material on the internet is protected by copyright and must be treated appropriately and in accordance with the owner's rights.

You must not copy, download or plagiarise material on the internet unless the owner of the website expressly permits you to do so.

The ICT Support Team Staff will provide appropriate Internet Filtering, staff must ensure that whilst in the school environment, all users do not visit internet sites, make, post, download, upload or pass on material, remarks, proposals or comments that contain or relate to:

- pornography (including child pornography);
- terrorism and extremist material
- promoting discrimination of any kind;
- promoting racial or religious hatred;
- promoting illegal acts;
- any other information which may be offensive to colleagues.

The school expects all users to use the internet responsibly and strictly according to the conditions above, and therefore all school devices will be subject to webfiltering and periodic monitoring checks to determine whether the internet browsing history has not contravened the terms of this policy and have been used appropriately.

Where inappropriate material appears to have been accessed (whether accidentally or not) staff should immediately report this to the Head of School or in their absence a member of the Senior Leadership Team so that appropriate action can be taken swiftly. This may include reviews with parents /carers.

Incidents which appear to infer deliberate access to web sites, newsgroups, social media sites and online groups that contain the following material will be reported to the police:

- images of child abuse (images of children, apparently under 16 years old) involved in sexual activity or posed to be sexually provocative;
- adult material that potentially breaches the Obscene Publications Act in the UK;
- criminally racist material in the UK.

5. Data Protection and System Security

User personal and system security code of conduct:

- Members of staff should never allow children to logon using their details.
- When entering personal details on a website login or the school network, if requested users should only save their details if they are using a device dedicated to their sole use, or if they are using their own personal computer.
- The staff shared area contains secure student detail and staff documentation. If users suspect that their details may have been compromised (seen by another person), they should change their password immediately.
- If accessing school data from home, school laptops that have been encrypted should always be used, not unencrypted removable media . Staff personal computers can be used providing they have up to date antivirus and data is only accessed when using the schools secure remote access system, no data should be stored on personal devices. Users should always ensure, by following the aforementioned code, that data integrity is respected at all times. Users should remember that school equipment and mobile technology is more vulnerable once it leaves the building, and susceptible to theft and loss along with its data.
- Regularly delete material you no longer require and to archive material that you wish to keep. For further information please see the Records Management Policy. Confidential emails should be deleted when no longer required.
- Ensure that confidential emails are always suitably protected. If working at home or remotely, you should be aware of the potential for an unauthorised third party to be privy to the content of the email.

6. Digital Media

Digital media and photographs play an important part of recording events in school life. School provides the capability for still and video digital images to be captured by children and staff. Staff should not use their own (personal) cameras or mobile phones to record identifiable images of children or staff. Any photographs or videos that are recorded and wish to be kept should be stored in a designated area on the school's network, and remain in school.

7. Staff and Governor Email

All email messages should include a standard disclaimer stating that the content of the email are confidential, and not necessarily the views of school. The appropriate ICT Support Team will provide details of the disclaimer content. Unsolicited email with children is not permitted. On no occasion should staff release or in any way make available personal details of any colleague or child (phone numbers, fax numbers or personal e-mail addresses) over the Internet.

Staff, Governors, Trustees and Members should only use the school's email system for work related emails.

As with anything else sent over the internet, emails are not completely secure. There is no proof of receipt, emails can be 'lost', they can suffer from computer failure and a determined 'hacker' could intercept, read and possibly alter the contents.

Staff must not install program files or non-business documents from external sources on to the school's network. This might happen by opening an email attachment or by downloading a file from a website.

If you have any reason for suspecting that a virus may have entered the school's system, you must contact ICT support staff responsible for the school immediately.

As with other methods of written communication, you must make a judgment about the potential damage if the communication is lost or intercepted. Never send bank account information, including passwords, by email.

Emails constitute records of the school and are subject to the same rules, care and checks as other written communications sent by the school.

Emails should be checked under the same scrutiny as other written communications.

Staff members should consider the following when sending emails:

- Whether it is appropriate for material to be sent to third parties
- The emails sent and received may have to be disclosed in legal proceedings
- The emails sent and received maybe have to be disclosed as part of fulfilling an SAR (Subject Access Request)
- Whether any authorisation is required before sending
- Printed copies of emails should be retained in the same way as other correspondence, e.g. letter
- The confidentiality between sender and recipient
- Transmitting the work of other people, without their permission, may infringe copyright laws.
- The sending and storing messages or attachments containing statements which could be construed as abusive, libelous, harassment may result in disciplinary or legal action being taken.

8. Business Email Etiquette

Staff members should follow these basic rules of business email etiquette:

- Include a clear, direct subject line. - Examples of a good subject line include "Meeting date changed," "Quick question about your presentation," or "Suggestions for the proposal."

- Use a professional email address. - Your work email address always conveys your name so that the recipient knows exactly who is sending the email.

- Think twice before hitting 'reply all.' - Refrain from hitting "reply all" unless you really think everyone on the list needs to receive the email.

- Consider using a signature block appropriate to the intended recipient. - Provide your reader with some information about you, this would state your full name, title, the company name, and your contact information, including a phone number.

- Use professional salutations. - Don't use laid-back, colloquial expressions like, "Hey guys, or "Hi folks." Use Hi or Hello instead. Be careful about shortening anyone's name. Say "Hi Michael," unless you're certain he prefers to be called "Mike."

- Use exclamation points sparingly. - If you choose to use an exclamation point, use only one to convey excitement, they should be used sparingly in writing.

- Be cautious with humor. - Humor can easily get lost in translation without the right tone or facial expressions. In a professional exchange, it's better to leave humor out of emails unless you know the recipient well.

- Keep your writing professional and non-conversational. – Remember the basic purpose of emails is to transfer information from one person to another.

- Know that people from different cultures speak and write differently. - Miscommunication can easily occur because of cultural differences, especially in the writing form when we can't see one another's body language. Tailor your message to the receiver's cultural background or how well you know them.

- Reply to your emails--even if the email wasn't intended for you. - It's difficult to reply to every email message ever sent to you, but you should try to, this includes when the email was accidentally sent to you, especially if the sender is expecting a reply. Here's an example reply: "I know you're very busy, but I don't think you meant to send this email to me and I wanted to let you know so you can send it to the correct person."

- Proofread every message. - Don't rely on spell-checkers. Read and re-read your email a few times, preferably aloud, before sending it off.

- Add the email address last. - This avoids sending the email accidentally before you have finished writing and proofing the message. Even when you are replying to a message, it's a good precaution to delete the recipient's address and insert it only when you are sure the message is ready to be sent.

- Double-check that you've selected the correct recipient. - Pay careful attention when typing a name from your address book on the email's "To" line. It is easy to select the wrong name.

- Keep your fonts classic. - Your emails should be easy for other people to read, use 10 to 12 point, easy-to-read fonts such as Arial, Calibri, or Times New Roman and black writing is best for clarity.

- Keep a careful eye on your tone. - Just as jokes get lost in translation, tone is easy to misconstrue without the context you'd get from vocal cues and facial expressions. Read your message out loud before hitting send. If it sounds harsh to you, it will sound harsh to the reader.

- Nothing is confidential--so write accordingly. - ***Every*** electronic message leaves a trail. A basic guideline is to assume that others will see what you write, so don't write anything you wouldn't want everyone to see. Don't write anything that would be ruinous to you or hurtful to others.

Sending or storing messages or attachments containing statements which could be construed as improper, abusive, harassing the recipient, libelous, malicious, threatening or contravening discrimination legislation or detrimental to the is a disciplinary offence and may also be a legal offence.

9. Mobile Phones & Watches/Other devices with phone call capability

Children are not allowed mobile phones or other devices with the ability to make telephone calls or access the internet in school during the course of the school day. These devices should be handed to the school office first thing in the morning for safekeeping if they are brought into school. Staff mobile phones should not be used during class times.

10. Internet Games

If There are times in the week when children have less restrictive use of the school network, such as during computer clubs, wet playtimes, reward time for good behaviour etc. Any games played on the school network must be in line with the school Code of Conduct, Safeguarding policy and e-Safety policy and be age appropriate the students.

11. Downloading Music

Students should not download music onto the school network. Staff may download music but this must be done legally and in line with copyright laws and the terms of this policy.

12. Internet Safety Skills for Children

E-Safety forms part of the school's curriculum and is taught implicitly to all age groups. Examples of topics taught relating to E-Safety include:

- how to critically evaluate materials;
- good searching skills;
- the importance of intellectual property regarding materials they find on the internet.

13. School Website

Any work published on the school website is thoroughly checked to ensure that there is no content that compromises the safety of children or staff. The school will obtain parental permission before using images of children on the website.

We ensure image files are appropriately named – i.e. do not use children's names in image file names or ALT tags if published on the web. This reduces the risk of inappropriate, unsolicited attention from individuals outside the school. Images will be appropriately stored and secured on the school's network.

Where staff and governors are issued with restricted access to resources and / or information within the school's network (via the school website), usernames and passwords must not be shared with or used by any other individual.

14. Agreement

All staff, governors and volunteers (where appropriate) are required to sign a copy of the respective Code of Conduct agreements that apply for the use of ICT Equipment (Appendix 1) and iPads (Appendix 2). The agreements ensure that members of staff, governors and volunteers are fully aware of and comply with the expectations of their professional responsibilities when using information systems and when communicating with children.

15. Sanctions

Any breaches of the policy by members of staff will be sanctioned in line with school policy. Breaches of the policy by governors and volunteers will fall under the discretion of the Head of School and Chair of the Governing Board/Chair of Trust where relevant.

Appendix 1 – Code of Conduct for ICT

To ensure that members of staff, governors and volunteers are fully aware of their professional responsibilities when using information systems and when communicating with children, staff are asked to sign this Code of Conduct. Members of staff should consult and familiarise themselves with the school's e-Safety and Safeguarding policies for further information and clarification.

The Agreement:

- I understand that it is a criminal offence to use any school ICT resource for a purpose not permitted by the Education Learning Trust, and that the school's digital technology resources and systems must not be used for personal or private business.
- I understand that ICT includes a wide range of systems, including mobile phones, tablets, laptops, digital cameras, email, social networking and agree to not use any personal ICT devices e-mails or networking sites in the school setting for activities which would contravene the values of the school.
- I understand that the use of my own (personal) device in school is only permitted with the express permission of the Head of School (or their delegated representative), and may otherwise constitute a breach of the school's network security and / or images consent policy. I accept that photographs or videos of children must not be taken or stored using any non-school device.
- I accept responsibility for any ICT equipment in my care and will ensure that it is returned to its correct place when being charged or not in use.
- When I take ICT equipment off site I will ensure that procedures and policies, to ensure integrity of data and information, are adhered to, including keeping equipment safe and not left unattended when off site (for example in unattended vehicles)
- I understand that neither the school digital technology resources, nor the content held within its information systems may be used for private or personal purposes without the express permission of the Head of School and Governing Body.
- I understand that my use of school information systems, internet and email may be monitored and recorded to ensure policy compliance.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure it is change at my earliest opportunity. I respect system security and I will not disclose any password or security information to anyone other than an authorised school representative (with responsibility for system / network management).
- I will not allow unauthorised individuals to access email, internet, or any school network or system I have access to. I will not allow anyone to login using my own login details and will ensure that I log off or lock the screen of any computer I am using [CTRL+ALT+DEL] or Window button & L if I leave the room.
- I will not download or install any software (including toolbars) or hardware without permission of an authorised school representative (with responsibility for system / network management).
- I will ensure all documents, data etc., are printed, saved, accessed and deleted in accordance with the Trust's data protection policies.
- I will ensure any documents containing sensitive information will be password protected before emailing, I will contact the email recipient via phone to share this password. Passwords should not be shared via email.

- I will not write or share my password with anyone. If I feel my password has been compromised I will contact the ICT staff responsible for the network immediately.
- I will only use age-related, designated search engines with children and will supervise children using the internet at all times.
- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of children or staff and will not store any such images or videos at home.
- I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff within the school network.
- I will ensure that personal data, including photographs, are stored securely and used appropriately, whether in school, taken off the school premises or accessed remotely when data is being physically transported, password protected folders etc.).
- I will respect copyright and intellectual property rights, and not use or copy copyright protected files without the correct authorisation.
- I will report any incidents of concern (whether intentional or accidental) regarding children's safety or inappropriate use of computers, ICT devices or the internet to the Head of School, or a member of the Senior Leadership Team in their absence.
- I will ensure that any electronic communication with parents and children including email, instant messages and via the school website (password protected access) are in keeping with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will only access school resources remotely (such as from home) using the school/ICT contractor approved system (password protected access) and follow e-security protocols to interact with them.
- I am aware of the rules for computer and internet usage for children, and will promote e-safety with children in my care - helping them to develop a responsible attitude to system use, communications and publishing.
- I understand that it is my duty to support a whole-school safeguarding approach and will report any behaviour (of other adults or children), which I believe may be inappropriate or concerning in any way, to the Designated Safeguarding Lead (or a senior member of staff in their absence).
- I will report any faults, malfunctions or suspected viruses including those that may be attached to emails, to the contracted ICT support staff, including full details and all error messages, as soon as possible..
- I will not store any sensitive data containing persona and special category data on any unencrypted media, on local non networked drives or non-sanctioned cloud storage
- I will not use email to access or send offensive material, chain messages or list-servers or for the purposes of bullying or plagiarising work.
- I will not send personal or inappropriate information by email about yourself, other members of staff, children or other members of the school community.

- I will not use a personal email address for school, Trust or governance communications and will only use my school or Trust issued email address.

- I have read, understood and will comply with the rules of business email etiquette contained in the ELT ICT Acceptable Use Policy.

The school may exercise its right to monitor the use of the school's information systems, devices and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system or content may be taking place; or that the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Signature

I have read, understood and accept the Code of Conduct for ICT. I agree to abide by all the points above. I understand that I have a responsibility for my own and others e-safeguarding and I undertake to be a 'safe and responsible digital technologies user'. I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies. I understand that failure to comply with this agreement could lead to disciplinary action.

Signed on behalf of the School/Trust	
Date	
Signed by employee/governor/trustee/volunteer/other	
Date	

Appendix 2 – Code of Conduct for Apple iPads

To ensure that members of staff, governors and volunteers are fully aware of their professional responsibilities when using school iPads, they are asked to sign this Code of Conduct. All parties should consult the schools' e-Safety and Safeguarding policies for further information and clarification.

- I understand that iPads remain the property of the school, and will need to be returned at the termination of my contract of employment (as appropriate).
- I will only use the iPad for school related business as detailed within this ICT Acceptable Use policy.
- I will only login to the Apple 'App store' and other subscription based services using my designated Apple ID and school email address only.
- I understand that it is my responsibility to keep the iPad secure and in good working order. In particular, I will ensure the iPad is kept safe when not on the school premises. (and for example, not left in an unattended vehicle)
- I will inform the school office immediately, upon any loss, theft, damage or destruction of the iPad.
- Any purchases made through the Apple iTunes account allocated to the iPad will be made using the correct purchasing procedures – i.e. using school issued iTunes gift certificates, and not personal credit cards and / or bank accounts.

The school may exercise its right to monitor the use of school iPads at any time.

Signature

I have read, understood and accept the Code of Conduct for ICT for using school iPads. I agree to abide by all the points above. I understand that I have a responsibility for my own and others e-safeguarding and I undertake to be a 'safe and responsible digital technologies user'. I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies. I understand that failure to comply with this agreement could lead to disciplinary action.

Signed on behalf of the School/Trust	
Date	
Signed by employee/governor/trustee/volunteer/other	
Date	