Document Owner and Approval

Evelina Hospital School is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with School's policy review schedule.

A current version of this document is available to all members of staff Staff shared drive and a copy in the school handbook.

Signature: Date:

Change History Record

Version	**Description of Change**	**Date of Policy Release by Judicium**
1	Initial Issue	06.05.18
2	Corrected spelling of iPads. Added bullet point about emails not containing personal opinions about other individuals and descriptions must be kept in a professional and factual manner.	23.08.19
3	Use of WhatsApp.	15.03.22

ACCEPTABLE USE POLICY AND AGREEMENT

This policy is designed to enable acceptable use for staff and governors.

The School provides a range of ICT resources which are available to staff members and governors. In order to ensure the safety of staff, governors and pupils, it is important that all staff members and governors follow the guidelines detailed below.

This policy aims to:

- Promote the professional, ethical, lawful and productive use of the School’s ICT systems and infrastructure.
- Define and identify unacceptable use of the School’s ICT systems and external systems.
- Educate users about their data security responsibilities.
- Describe why monitoring of the ICT systems may take place.
- Define and identify unacceptable use of social networking sites and school devices.
- Specify the consequences of non-compliance.

This policy applies to staff members and governors, and all users of the School’s ICT systems are expected to read and understand this policy. To confirm acceptance of the policy, users will sign an Acceptable Use Agreement which is attached to this policy. Breach of this policy may result in disciplinary action.

The use by staff and monitoring by the School of its electronic communications systems is likely to involve the processing of personal data and is therefore regulated by the Data Protection Act 2018, together with the Employment Practices Data Protection Code issued by the Information Commissioner. Staff are referred to the School's Data Protection Policy for further information.

If you are in doubt and require clarification on any part of this document, please speak to Headteacher.

Provision of ICT Systems

All equipment that constitutes the School’s ICT systems is the sole property of the School.

No personal equipment should be connected to or used with the School’s ICT systems. Users must not try to install any software on the ICT systems without permission from Headteacher. If software is installed without permission, it may cause extensive damage to the ICT systems and users could be held personally liable for any costs incurred in rectifying the damage.

Headteacher is responsible for purchasing and/or allocating ICT equipment to individuals. Individual laptops/desktop computers or ICT equipment may be removed at any time, without prior warning, for regular maintenance, reallocation or any other operational reason. Maintenance includes, but is not limited to, new software installations, software updates, reconfiguration of settings and computer re-imaging.

Users are not permitted to make any physical alteration, either internally or externally, to the School's computer and network hardware.

Network Access and Security

All users of the ICT systems at the School must first be registered. Following registration, a network user account will be created, consisting of a username, password and an e-mail address. All passwords should be of a complex nature to ensure data and network security. All user account details are for the exclusive use of the individual to whom they are allocated. Staff are responsible for ensuring their password remains confidential and their account is secure. Passwords must be regularly changed.

All users are personally responsible and accountable for all activities carried out under their user account(s). Users must take all reasonable precautions to protect their user account details and must not share them to any other person, except to designated members of the IT consultant for the purposes of system support. Users must report any security breach or suspected breach of their network, email or application account credentials to the School Business Manager as soon as possible.

Users should only access areas of the Schools computer systems to which they have authorised access.

When any computer is left unattended, it must either be logged off or locked. Activity that threatens the integrity of the School ICT systems, or activity which attacks or corrupts other systems, is forbidden. Users' internet activity must not compromise the security of the data on the School ICT systems or cause difficulties for any other users.

Under no circumstances should a pupil be allowed to use a staff computer account, unless being directly supervised by the account owner.

School Email

Where email is provided, it is for academic and professional use, with reasonable personal use being permitted. Personal use should be limited to short periods during recognised break times and comply with this Acceptable Use policy. The School's email system can be accessed from both the School computers, and via the internet from any computer. Wherever possible, all School related communication must be via the School email address.

The sending of emails is subject to the following rules:

- Language must not include swear words, or be offensive or abusive.

- Emails or attachments of a pornographic, illegal, violent, sexist or racist nature are not permitted.
- Sending of attachments which contain copyright material to which the School does not have distribution rights is not permitted.
- The use of personal email addresses by staff for any official school business is not permitted.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) will only be sent using a secure method including:
  - Email encryption;
  - A secure upload portal (where by the recipient will be required to log in to retrieve the email/documentation sent);
  - Password protection on sensitive documents. The sender must ensure that the password is sent separately to the intended recipient (i.e. in a separate email or over the phone).
- Emails should not contain children's full names in the subject line and preferably, not in the main body of the text either. Initials should be used wherever possible.
- Access to school/setting email systems will always take place in accordance to data protection legislation and in line with other appropriate school/setting policies e.g. confidentiality.
- Members of the community must immediately tell a designated member of staff if they receive offensive communication, and this will be recorded in the relevant files/records (such as safeguarding).
- Staff will be encouraged to develop an appropriate work life balance when responding to email.
- Emails sent to external organisations should be written carefully and checked before sending, in the same way as a letter written on school headed paper would be.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.
- Where possible, emails must not contain personal opinions about other individuals, e.g. other staff members, children or parents. Descriptions of individuals must be kept in a professional and factual manner.

Internet Access

Internet access is provided for academic and professional use, with reasonable personal use being permitted. Priority must always be given to academic and professional use.

The School's internet connection is filtered, meaning that a large amount of inappropriate material is not accessible. However, on occasions it may be possible to view a website which is inappropriate for use in a school. In this case the website must be reported immediately to the Headteacher.

Staff must not therefore access from the School's system any web page or any files downloaded from the web which could be regarded as illegal, offensive, in bad taste or immoral.

Misuse of the internet may, in certain circumstances, constitute a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet by viewing, accessing, transmitting or downloading any of the following material, or using any of the following facilities, will amount to gross misconduct (this list is not exhaustive):

- accessing pornographic material (that is writings, pictures, films, video clips of a sexually explicit or arousing nature), racist or other inappropriate or unlawful materials;
- transmitting a false and/or defamatory statement about any person or organisation;
- sending, receiving, downloading displaying or disseminating material which is discriminatory, offensive, derogatory or may cause offence and embarrassment or harass others;
- transmitting confidential information about the School and any of its staff, students or associated third parties;
- transmitting any other statement which is likely to create any liability (whether criminal or civil, and whether for the employee or for the School);
- downloading or disseminating material in breach of copyright;
- engaging in online chat rooms, instant messaging, social networking sites and online gambling;
- forwarding electronic chain letters and other materials;
- accessing, downloading, storing, transmitting or running any material that presents or could present a risk of harm to a child.

Any such action will be treated very seriously and may result in disciplinary action up to and including summary dismissal.

Where evidence of misuse is found, the School may undertake a more detailed investigation in accordance with our Disciplinary Policy, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or members of management involved in the disciplinary procedure.

If necessary, such information may be handed to the police in connection with a criminal investigation.

Digital Cameras

The School encourages the use of digital cameras and video equipment. However, staff should be aware of the following guidelines:

- Photos should only have the pupil’s name if they are on display in school only. Photos for the website or press must only include the child’s initials.
- The use of personal digital cameras in school is not permitted, including those which are integrated into mobile phones, iPads or similar.
- All photos should be downloaded to the School network as soon as possible.

- The use of personal mobile phones for taking photos of pupils is not permitted.

File Storage

Staff members have their own personal area on the network, as well as access to shared network drives. Any school related work should be stored on one of these network drives. Personal files are not permitted on the network areas. Staff are responsible for ensuring they have rights for the storage of any file in their area, for example copyright music files. Any files stored on removable media must be stored in accordance with the Information Security Policy, summarised as follows:

- If information/data is to be transferred, it must be saved on an encrypted, password protected, storage device.
- No school data is to be stored on a home computer, or un-encrypted storage device.
- No confidential, or school data which is subject to the Data Protection Act should be transferred off site unless it is sent by secure email.

Mobile Phones

Mobile phones are permitted in school, with the following restrictions:

- They are not to be used when members of staff are directly supervising or working with children. Whilst members of staff are working in the classroom they should be securely stored in a bag or cupboard.
- Personal mobile phone cameras are not to be used. The School provides digital camera and ipads for this purpose.
- All phone contact with parents regarding school issues will be through the School’s phones. Personal mobile numbers should not be given to parents at the School.

Use of Whatsapp

WhatsApp is not permitted for use on personal devices for School business. Members of staff are able to use WhatsApp on their own devices for personal communication however, staff should not communicate internally with other staff members for School business using their personal WhatsApp accounts, sharing School related information which could include categories of personal data. Staff should communicate via Microsoft Teams or school emails for school business.

Microsoft Teams and other Video Conferencing Facilities

Staff members have their own Microsoft Teams account and are strongly recommended to use this platform when using video conferencing adhering to the following guidelines:

- Ensure you have a complex password to access the system

This means having a mixture of numbers, letters, capitals and possibly special characters.

- Do not access video conferencing facilities on a personal mobile phone

As well as being impractical (as you may not be able to see all users on a mobile device), there have been instances of video conferencing software sharing data with social media channels (such as Facebook) without permission.

- Do not record calls without prior permission.

We need consent to record users so permission should be sought at the beginning of a call. In any event video recordings should not be taken unless absolutely necessary and you should seek permission from the Headteacher before doing so.

- Check all the correct participants are present on the video call

Although unlikely, it can be possible for unauthorised individuals to jump on video calls. It may be best to start the call with a register if many users are involved on the call. Where confidential meetings are taking place, the participant must find a secure space to do so and must declare to the other parties if there other people present.

- Ensure settings are fixed so that other users on the call cannot record the conversation covertly.

Check the system's settings to ensure that other users can't record calls. Also remind users at the beginning that the call should not be recorded.

- External links shouldn't be shared

A lot of video conferencing software isn't encrypted and so can be prone to hacking. This can allow unauthorised users to join calls and send links to others (and these links when opened may expose user's account details and passwords). At the beginning of a call it may be beneficial to remind users not to open any external links sent over chat.

- Sensitive documents shouldn't be shared over video call

Screen share facilities should be used rarely and should contain no personal data where possible. Other users can click "print screen" and then have a copy of documents they may not be entitled to. Additionally, unauthorised third parties external to the call may be able to access this data.

- Do not send chat logs

If you send the chat log at the end of a call to users, you could be sending data they are not entitled to see. Some chat logs include private messages on them so beware sending chat logs to others.

- Take control of the meeting

It is always best to have a facilitator to run the meeting, set the ground rules (such as making it clear there is to be no recording, etc) and also to set rules on chat etiquette (such as asking them to raise their hand before speaking).

- Limit sending private or "side" messages to users

Content should be available to all.

- Preparation/follow up

If you need to send documents or work in advance or following a chat session, do ensure that (1) all users are blind copied (BCC) into the email and (2) to avoid sending any sensitive data in those emails. If you need to send sensitive data (such as health data) to a specific individual, do re-check the email address before sending to check it is being sent to the correct recipient.

- Do not give out personal email addresses and numbers to users. Only school email addresses should be provided.

Providing personal details such as phone numbers, social media accounts or email addresses are forbidden in any circumstances. Please ensure you only provide them with official work communications only.

- If you want to implement new software to interact with students, please let your line manager know.

We need to conduct a data protection impact assessment before using them. Whilst there are lots of creative ways to communicate and interact with others during these times, some of those technologies are relatively untested so we as a company need to consider any security risks to data. Please do ask your line manager in the first instance.

Home Working

Staff may be required to work remotely and should ensure they follow good practice when doing so, including:-

- Ensuring sensitive data is secured away and not shared with family and friends.
- Only using school devices and not personal devices.
- To avoid sharing personal data of third parties with others.
- To secure away any work devices safely.

Staff should familiarise themselves with the Guidance Notes for "Staff on Working From Home" for acceptable practice when working from home.

The School has a Social Media Policy which should be read in conjunction with this policy.

Social Networking

The key requirements for staff are as follows:

- Staff members have a responsibility to protect the reputation of the School, staff and students at all times and must treat colleagues, students and associates of the School with professionalism and respect whilst using social networking sites.
- Social networking sites should be used responsibly, and users should ensure that neither their personal or professional reputation and/or the School's reputation, nor the reputation of individuals within the School are compromised by inappropriate postings.
- Use of social networking sites for school business is not permitted, unless via an officially recognised school site and with the permission of the Headteacher.
- Members of staff will notify the Headteacher if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the School/setting.
- No school information, communication, documents, videos and/or images should be posted on any personal social networking sites.
- No details or opinions relating to any pupil are to be published on any website.
- Users must not knowingly cause annoyance, inconvenience or needless anxiety to others (cyber bullying) via social networking sites.
- No opinions regarding another member of staff, which could cause offence, are to be posted.
- No photos or videos, which show pupils of the School who are not directly related to the person posting them, should be uploaded to any site other than the School's Website.
- No comment, images or other material may be posted anywhere, by any method that may bring the School or, the profession into disrepute.
- Users must not give students access to their area on a social networking site, (for example adding a student as a friend on Facebook). If, in exceptional circumstances, users wish to do so, please seek advice from Headteacher.

Monitoring of the ICT Systems

The School may exercise its right to monitor the use of its ICT systems. This includes websites accessed, the interception of e-mail and the viewing of data stored, where it believes unauthorised use of the School's ICT system is, or may be taking place, or the system is, or may be being used for criminal purposes. Any inappropriate material found will be deleted. The use of the network is regularly checked by the IT consultant under the direction of the Headteacher to ensure there are no pastoral or behaviour concerns or issues of a safeguarding or prevent nature.

Other reasons for monitoring the ICT systems include the need to:

- ensure operational effectiveness of the services provided;
- maintain the systems;
- prevent a breach of the law, this policy, or any other school policy;
- investigate a suspected breach of the law, this policy, or any other school policy.

Failure to Comply with Policy

Any failure to comply with the policy may result in disciplinary action. Depending upon the severity of the offence, a breach of this policy may be considered gross misconduct leading to summary dismissal.

Any unauthorised use of the School's ICT systems, Cloud-based ICT systems, the internet, e-mail and/or social networking site accounts, which the Headteacher considers may amount to a criminal offence or is unlawful shall, without notice to the user concerned, be reported to the police or other relevant authority.

The School reserves the right to audit and/or suspend a user's network, e-mail and/or application account(s) pending an enquiry, without notice to the user concerned.

ACCEPTABLE USE AGREEMENT

To be completed by all staff

As a school user of the network resources/equipment I hereby confirm that I have read and understood the Acceptable Use Policy and that I agree to follow the School rules (set out within this policy) on its use. I will use the network/equipment in a responsible way and observe all the restrictions explained in the School Acceptable Use Policy. If I am in any doubt, I will consult the Headteacher.

I agree to report any misuse of the network to the Headteacher. Moreover, I agree to report any websites that are available on the School internet that contain inappropriate material to the Headteacher. I finally agree to ensure that portable equipment such as cameras, iPads or laptops will be kept secured when not in use and to report any lapses in physical security to the Headteacher.

Specifically, when using school devices:

- I must not use these devices for inappropriate purposes;
- I must only access those services for which permission has been granted;
- I will not download, use or upload any material which is unsuitable within a School setting or that may cause disruption to the School network.

If I do not comply with the rules, I understand that this may result in loss of access to these resources as well as other disciplinary action. I realise that staff under reasonable suspicion of misuse in terms of time or content may be placed under retrospective investigation or have their usage monitored.

I understand that my school email may be redirected to a member of the admin team to manage school correspondence during any prolonged absence.

I understand that the School will monitor communications in order to uphold this policy and to maintain the School’s network (as set out within this policy).

Signed ………………………………………………………………………………………….. Date …………………………….

Print name ……….