Redmaids' High School
Staff ICT Acceptable Use

REDMAIDS' HIGH SCHOOL
FOR GIRLS | BRISTOL
SENIOR SCHOOL & SIXTH FORM

This Acceptable Use Agreement is usually sent via Operoo to all staff who have access to School IT equipment. In some cases, staff will be asked to sign a hard copy of this form. Staff are asked to sign to say they agree with the policy on joining the School and at the start of the new school year.

Introduction

This policy sets out the requirements with which you must comply when using the School's IT systems and equipment (including your own devices) in connection with your job including:

- the School's email and internet services;
- telephones;
- the use of mobile technology on School premises or otherwise in the course of your employment (including 3G / 4G or Bluetooth or other wireless technologies), whether using a school or a personal device (to include the use of WhatsApp and other technology based communications); and
- any hardware (such as laptops, printers or mobile phones) or software provided by, or made available by, the School or otherwise used in connection with your job.

This policy also applies to your use of IT off school premises if the use involves Personal Data of any member of the School community or where the culture or reputation of the School are put at risk.

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 including students.
- I recognise the value of the use of ICT for enhancing learning and will ensure that students receive opportunities to gain from the use of ICT.
- I will, where possible, educate the students in my care in the safe use of ICT and embed e-safety in my work with the students.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email, file storage and other digital communications.

- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. iPads, email, Virtual Learning Environment (VLE) etc.) out of school, during remote learning and when using a personal device.
- I understand that the school ICT systems and equipment are for educational use primarily, my personal use should be kept to a minimum and should not interfere with work commitments.
- 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 Melissa Stimson or Lisa Brown, who are the Designated Safeguarding Leads or to Alice Hinks who is the Online Safety Officer or any other appropriate member of staff.

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 will demonstrate and 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.
- Where images are published (e.g. on the school website/Twitter feed) it will not be possible to identify those who are featured by their full name, or other personal information.
- I will only use chat and social networking sites in school in accordance with the social media code of practice.
- I will keep my private social media accounts on the highest privacy settings to prevent them being accessed by students.
- I will only communicate with students and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will not use my school email address for personal matters

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

- 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 any data that I work on locally on my iPad is regularly saved into a secure school cloud folder and ensure it is regularly backed up and appropriately secured.
- I will not try to upload, download or access any materials which are illegal (e.g. 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 monitoring and filtering security systems in place to prevent access to such materials.
- I will not attempt to transfer 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.
- I will not disable or cause any damage to school equipment or the equipment belonging to others.
- I understand that in line with Data Protection (UK GDPR) there are a number of associated policies which outline the requirement 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. These policies are:
    - Parent Privacy Notice
    - Pupil Privacy Notice for Parents of Junior School Pupils
    - Student Privacy Notice for Senior School Students
    - Staff Privacy Notice
    - Visitor Privacy Policy
    - Information and Records Retention Policy
    - Data Protection Policy
    - Taking, Storing and Using Images of Pupils Policy

- I will immediately report any damage or faults involving equipment or software, however this may have happened, to IT.

- I will not enter into any contract or subscription on the internet (including through an App) on behalf the School, without specific permission from IT and the DFO. This applies both to "free" and paid for contracts, subscriptions and Apps.

- I understand that when engaging the services of an App or cloud-based service that is processing personal data that, with the engagement of IT Support, we ensure that they use appropriate technical and organisational measures, by inspecting their Data Protection or privacy policies. I will also inform the Compliance Officer to ensure the service or App is logged on our IT Systems and Apps Register.

- I understand that the use of USB sticks to transfer personal and confidential data is prohibited unless the storage device has been encrypted or pseudonymisation has been carried out by IT Support.

- I will report any and all breaches of personal data in line with the school's Data Breach Policy. The Data Breach Policy should be read in conjunction with this document.

- I understand that if I borrow a device from ICT that I must sign out of all applications before returning it. I will ensure that it is returned to a member of the IT staff so that the device can be checked before it is loaned out again.

- I understand that when I am using a personal device (PC, laptop or tablet) I will:

    - Log out when I leave my device and close the browser, especially if I share the device with a family member
    - Turn off my microphone when I finish a live session – if I am delivering remote learning
    - Ensure my device is password protected
    - Not save any school data on my personal device and check my download folder does not hold any school data
    - Not ignore the Windows or Mac upgrades as they have important security patches
    - Ensure the Outlook app is kept up-to-date on mobile phones
    - Ensure virus protection on my PC or laptop is up-to-date – Bitdefender has a free version
    - Not access school systems using free unsecured WiFi or VPNs
    - Not log into a device that is not owned by me
    - Not send sensitive information over email – I will save it in OneDrive and share access that way. If I need help with this, I will contact a Digital Leader (or equivalent in the Junior School)
    - Contact the Compliance Officer or IT as soon as possible if my device is stolen, hacked or I think someone has accessed school data.

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 or termination of employment in line with the school's disciplinary procedures. In the event of illegal activities, the school may involve the Police.

Sarah Bramley-Dymond/Elizabeth Fry/Bisola Ezobi
Reviewed Summer term 2023
Next review Summer term 2024

I have read and understand the Staff ICT Acceptable Use Agreement 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.

Signed ----------

Name ----------

Date ----------