Downe House
Riyadh

e-Safety Policy and ICT Acceptable Use Agreements

This policy applies to all staff, pupils, parents, and visitors in the school.

Table of Contents

1. Introduction

Downe House Riyadh acknowledges that the use of the internet and mobile devices have become fully integrated into the lives of young people. Furthermore, the staff value the contribution that electronic devices can make to support learning and the wealth of opportunities that they provide in furthering a child's education. Downe House Riyadh is aware that there are online risks and sometimes these risks can lead to harm; therefore, this e-safety Policy applies to all pupils, staff, parents, support staff, external contractors and members of the wider community who use, have access to or maintain school or school-related internet and computer systems.

To ensure that both pupils and staff are protected and are aware of what is deemed as inappropriate behaviours, these rules have been put into place to ensure online safety. The e-Safety Policy is made available to the whole school community via the school website. Furthermore, the issues contained within the policy and areas such as online stranger danger, how to protect yourself on the internet and how to report suspicious activity are areas that are covered across the curriculum, during assemblies and at school events where appropriate.

2. Roles and responsibilities

2.1 Senior Leadership Team

The Senior Leadership Team (SLT) is responsible for:

- Determining, evaluating, and reviewing e-Safety policies to encompass teaching and learning and the use of Downe House Riyadh IT equipment and facilities by pupils, staff and visitors.
- Regularly updating the e-Safety policy, child protection policy and ensuring that e- Safety incidents are logged and evaluated.
- Staff inset provision.
- Working closing with ICT manager to ensure e-Safety policy is met.

2.2 The ICT Manager

The ICT manager (along with all staff) is responsible for:

- e-Safety issues on a day-to-day basis.
- Maintaining a log of submitted e-Safety reports and incidents.
- Auditing and assessing inset requirements for staff, support staff and e-Safety training, and ensuring that all staff are aware of their responsibilities and Downe House Riyadh 's e-Safety procedures. The ICT Manager is also the first port of call for staff requiring advice on e-safety matters.
- Although all staff are responsible for upholding the school's e-Safety policy and safer internet practice, the ICT Manager is responsible for monitoring internet usage by pupils, staff and visitors on the school's devices.

2.3 ICT support staff and external contractors

Internal ICT support staff and technicians are responsible for maintaining the Downe House Riyadh networking, IT infrastructure and hardware, being aware of current thinking and trends in IT security and ensuring that the school's system, particularly file-sharing and access to the internet is secure. They need to further ensure that all reasonable steps have been taken to ensure that systems are not open to abuse or unauthorised external access, with particular regard to external logins and wireless networking.

ICT support staff also need to maintain and enforce the protection of the school's passwords and monitor and maintain the internet filtering system.

ICT support staff must ensure that external contractors, such as network providers, website designers/hosts/maintenance contractors are made fully aware of and agree to the school's e-Safety policy.

2.4 Teaching and teaching support staff

Teaching and teaching support staff need to ensure that they are aware of the current e-Safety policy, practices, and associated procedures for reporting e-Safety incidents.

Teaching and teaching support staff will be provided with e-Safety induction as part of the overall staff induction procedures.

All staff need to ensure that they have read, understood, and signed (thereby indicating an agreement) the acceptable use policies relevant to their role.

All teaching staff need to rigorously monitor pupil internet and computer usage in line with the policy. This also includes the use of personal technology such as iPads, cameras, phones and other gadgets on the school site.

Teaching staff should promote best practice regarding avoiding copyright infringement and plagiarism.
Internet usage and suggested websites should be pre-vetted before teaching the lesson.

2.5 Pupils

Pupils are required to use the school's internet and computer systems in agreement with the terms specified in the acceptable use policies. Pupils are expected to sign the policy to indicate agreement, and/or have their parents/guardians sign on their behalf.
Pupils need to be aware of how to report e-safety incidents.

Pupils need to be aware that the acceptable use policies cover all computer, internet and gadget usage in the school, including the use of personal items such as phones.

Pupils need to be aware that their internet use out of the school on social networking sites such as Facebook is covered under the acceptable use policy if it impacts on the school and/or its staff and pupils in terms of cyber bullying, reputation or illegal activities (please refer to anti bulling policy for further information).

2.6 Parents

It is hoped that parents and guardians will support the school's stance on promoting safe internet behaviour and responsible use of IT equipment both in school and at home.

Downe House Riyadh expects parents and guardians to sign the acceptable use polices, indicating agreement regarding their child's use and also their own use with regard to parental access to the school's systems such as websites, forums, social media, online reporting arrangement and questionnaires, and to be aware that their internet use out of the school on social networking sites such as Facebook is covered under the acceptable use policy if it impacts on the school and/or its staff and pupils in terms of cyber bullying, reputation or illegal activities.

2.7 Board Members

The Board member with responsibility for Safeguarding will also be responsible for e-safety, and the Principal

will liaise directly with the Governor with regard to reports on e-safety effectiveness, incidents, monitoring, evaluation and developing and maintaining links with local stakeholders and the wider School community.

2.8 The Acceptable Use Agreement must be read and signed by all staff members, pupils and parents.

3. Technological Requirements

The ICT Manager ensures that the school has a technical infrastructure that is secure and protected from malicious attack. The downloading of software by unauthorised users on school devices is prohibited. The ICT Manager is also responsible for keeping the electronic equipment, servers, and technical systems up to date and secure from unauthorised access and ensuring that any service provider must carry out all the schools e-Safety measures. Passwords are in place that limit and control access to the school network and devices and are changed yearly or sooner upon request from the Principal. Temporary 'Guest' logins are provided for temporary staff i.e., supply teachers and these passwords should be changed on a termly basis.

4. Password Security

Staff and pupils read and sign an acceptable use agreement to demonstrate that they have understood the school's e-Safety policy. Guests are required to agree to terms when registering to use the wireless network.

Pupils are not allowed to deliberately access on-line materials or files on the school network, belonging to their peers, teachers or others.

If you think your password may have been compromised or someone else has become aware of your password, you must report this to the ICT manager immediately.
Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks.

Due consideration should be given to security when logging into the school website browser/cache options (whether shared or on a private computer).

5. Data Security

The accessing of school data is something that the school takes very seriously. Staff are aware of their responsibility when accessing school data. They must not:

- Access data outside of school unless permission has been granted.
- Take copies of the data.
- Allow others to view the data.
- Edit the data unless specifically requested to do so by the Principal.

6. Managing the Internet

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education and a potential risk to young people. The school will regularly monitor the use of the internet within school and whenever any inappropriate use isdetected, it will be immediately followed up with the Principal.

The school ensures pupils have supervised access to internet resources (where reasonable) through the school's fixed and mobile internet technology. Staff will preview any recommended sites before use. Raw image searches are discouraged when working with pupils.

If internet research is set for homework, it is advised that parents check the sites and supervise the work. Parents will be advised to supervise any further research.

All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources. All users must also observe copyright of materials from electronic resources.

The school liaises with the Ministry of Education to help implement and promote the Safe Space policies to ensure children are safe on the internet.

7. Infrastructure

The ICT manager ensures that the firewall in place has a monitoring solution web filter where web-based activity is monitored and recorded.

School internet access is controlled through the firewalls web filtering service The school has the facility for additional web filtering which is the responsibility of the ICT manager.

Staff and pupils are aware that school-based email and internet activity can be monitored and explored further if required. The school does not allow pupils access to internet history.

If staff or pupils discover an unsuitable site, the screen must be switched off or closed and the incident reported immediately to the teacher who will then inform the ICT manager, ICT coordinator and Principal.

It is the responsibility of the school, by delegation to the network manager to ensure that anti-virus protection is installed on all school machines and remains up to date. If staff suspect a virus, they must contact the ICT manager immediately.

Pupils and staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems have up- to-date virus protection software. It is not the school's responsibility nor the network manager's, to install or maintain virus protection on personal systems.

Pupils are not permitted to download programs or files on school-based technologies without prior permission (this does not include pupils iPads).

8. Mobile Technologies Including iPads

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership of devices such as iPads. With these devices comes internet access and thus opens up risk and possible misuse associated with communication and internet use. Any emerging technologies will be examined for educational benefit and the risk will be assessed before use in school is allowed.

Our school chooses to manage the use of these devices in the following ways to ensure safe and appropriate use:

- The school allows staff to bring in personal mobile phones and devices for their own use. Under certain circumstances the school allows a member of staff to contact a pupil or parent/carer using their personal device, although such devices should be concealed or kept in a bag / desk at all times. Should a call need to be received or made, staff are advised to do so away from the working environment.
- The school is not responsible for the loss, damage or theft of any personalmobile device.
- The sending of inappropriate text messages between any member of the school community is not

allowed.

- Permission must be sought before any image or sound recordings are made on devices belonging to any member of the school community.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- Where the school provides mobile technologies such as phones, laptops and iPads for offsite visits and trips, only these devices should be used.

9. Managing Email

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, emails should not be considered as private.

Educationally, emails can offer significant benefits including direct written contact between schools on different projects, be they staff based or pupil based. We recognise that pupils need to understand how to style an email in relation to their age, report suspicious emails and how to send and receive appropriate emails.

The school issues all staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.

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. If necessary, email history can be traced.

Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses (this does not apply to class Mums / Dads).

E-mail sent to an external organisation should be written carefully beforesending, in the same way as a letter written on school headed paper would be written.

Staff should email parents through the iSAMS system for bulk class/set emails and if it is felt a record of the email should be held on the system.

Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.

All email users are expected to adhere to the generally accepted rules of network etiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in email communication.

All attachments must be scanned for viruses.

Pupils must immediately tell a teacher/ trusted adult if they receive an offensive email.

Staff must inform the ICT manager and their line manager if they receive an offensive email.

Pupils are introduced to email as part of the ICT curriculum.

10. Safe Use of Images & Taking of Images and Film

Digital images are easy to capture, reproduce and publish and therefore, be misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness of doing so.

The school permits the appropriate taking of images by staff and pupils with school equipment unless parents specify otherwise.

Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils; this includes when on field trips.

However, with the express permission of the Principal, images can be taken provided they are transferred

immediately and solely to the school's network, website and/or the school's social media pages before being deleted promptly from the staff device.

11. Consent of adults who work at the school

Permission to use images of all staff who work at the school is sought upon induction.

12. Publishing Pupil's Images and Work

On a child's entry to the school, all parents/guardians will be asked to give permission to use their child's work/photos in the following ways:

- On the school web site and social media accounts (Twitter, Facebook etc).
- In the school prospectus and other printed publications that the school may produce for promotional purposes.
- Recorded/ transmitted on a video or webcam.
- In display material that may be used in the school's communal areas.
- In display material that may be used in external areas, i.e. exhibition promoting the school.
- General media appearances, eg local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically) This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances and the school is informed of this in writing from the parent. Consent must be given by a parentor guardian in order for it to be deemed valid.
- Should an image of a child be used, only the first name will appear alongside it.
- E-mail and postal addresses of pupils will not be published.

13. Storage of Images

Images/ films of children are stored on the school network or the class teacher computer. Pupils and staff are not permitted to use personal portable media for storage of images (e.g. USB sticks) without the express permission of the Principal.

Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network.

The ICT manager has the responsibility of deleting the images when they are no longer required, or the pupil has left the school.

14. Webcams

We do not use publicly accessible webcams in school. Webcams in school are only ever used for specific learning purposes.

Misuse of the webcam by any member of the school community will result in sanctions (as listed under the 'inappropriate material' section of this document).

15. Video Conferencing

All pupils are supervised by a member of staff when video conferencing. Approval from the Principal is sought prior to all video conferences within school.

The school conferencing equipment is not set to auto-answer and is only switched on for scheduled and

approved conferences. No part of any video conference is recorded in any medium without the written consent of those taking part.

Complaints relating to e-Safety should be made to the ICT manager and the Principal.

16. Inappropriate Material

All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the ICT manager.

Deliberate access to inappropriate materials by any user will lead to the incident being logged by the Principal, depending on the seriousness of the offence; investigation will be held and could result in immediate suspension, possibly leading to dismissal and involvement of local authorities for very serious offences.

Users are made aware of sanctions relating to the misuse or misconduct on the acceptable use agreement.

17. Pupils with additional needs

Staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-Safety issues.

18. Social Media and Online Identities

18.1 For educational purposes, staff may wish to communicate with pupils or allow pupils to communicate with each other on official school sites via email or through related Apps. Downe House Riyadh does not allow staff to use social media sites or other personal accounts to communicate with pupils or parents. Downe House Riyadh will educate pupils on the safe use of social media e.g., utilising privacy settings and the cautionary sharing of personal information and photographs as well as the significance and consequences of their online behaviour, legal sanctions, and digital footprints. The school will also educate staff and pupils on the potential risks of viruses and malicious content through external initiatives.

18.2 Staff are not permitted to accept friend requests, followers or tags etc. from pupils on any personal social media accounts. If present employees receive such requests, they must discuss these in general terms within the class. Furthermore, it is advised that on leaving the school, staff members do not contact pupils on any social media site. Staff members are strongly advised that they set the privacy levels of their personal sites as strictly as possible and keep all passwords and personal information confidential. Staff must, at all times, act in the best interest of children and young people when creating, participating in or contributing content to social media sites.

18.3 If pupils, staff or parents identify themselves as members of the school community on social media pages, chatrooms or forums, they must act in a way that upholds the core values and rules of the school. This is to prevent negative information on these sites from being linked with Downe House Riyadh and to safeguard the privacy of the staff and pupil body. It should be noted that the school treats any abuse of its staff, pupils and reputation with the upmost seriousness and any member of the whole school community who is thought to be portraying the school negatively by acting in an unprofessional manner whilst online will be immediately reported to the Principal.

19. Access, Monitoring and Sanctions

To promote positive pupil behaviour, Downe House Riyadh ensures a demonstrable correlation between procedures and sanctions for pupils. Therefore, any pupil in breach of the e-Safety policy will follow necessary

sanctions. The school has enhanced user-level filtering procedures in place that allows different content to be accessed/denied depending on the year group or staff role. Emails, webpages and remote access are monitored and reviewed by the ICT Manager, who will update the Principal accordingly.

20. Reporting and Recording Safeguarding Concerns

The school will report and act on instances of cyber bullying, abuse, harassment, malicious communication and grossly offensive material in line with the Behaviour Policy, Safeguarding Policy and Anti-Bullying Policy and where appropriate parents will be informed.

21. e-Safety Incident Log

Details of all e-Safety incidents must be recorded by the ICT manager. This incident log will be monitored by the designated SLT line manager.

22. Review and Staff Development

22.1 This policy is to be reviewed by the ICT manager and School Leadership Team every two years or sooner if required. The e-Safety Policy will be reviewed on a termly basis by the ICT manager.

22.2 As required, the school will provide staff with relevant training which will allow them to confidently prevent and intervene in any e-Safety concerns.

23. Policy History

Date of adoption of this policy	September 2022
Date of last review of this policy	August 2024
Date for next review of this policy	August 2025
Policy owner (SLT)	Deputy Head (Pastoral)
Policy owner (the Board)	Chair

Downe House
Riyadh

ICT ACCEPTABLE USE AGREEMENT for PARENTS

Dear Parents,

Downe House Riyadh recognises that the use of the internet and mobile devices have become fully integrated into the lives of young people. Furthermore, the school values the contribution that electronic devices can make to support learning and the wealth of opportunities that they provide. It is hoped that parents and guardians will support Downe House Riyadh 's stance on promoting safe internet behaviour and responsible use of IT equipment bothin school and at home.

Parent/Carer Responsibilities - Devices

It is essential that the following guidelines be followed to ensure the safe, efficient, and ethical use of the device. As a parent/carer I will:

- I will supervise my child's use of the device at home.
- I will discuss our family's values and expectations regarding the use of the internet and email at home.
- I will supervise my child's use of the internet and email.

Parent/Carer Responsibilities - Online behaviour

At Downe House Riyadh , we encourage parents to ensure that any complaints are dealt with in a professional manner, by either contacting the class teacher, or, if necessary, arranging a meeting with a member of the Senior Leadership Team. We ask that parents do not use social media, chat forums or websites to discuss issues or concerns related to Downe House Riyadh . To ensure the safety of our staff and pupils, we ask that parents refrain from making reference to any member of our school community. Any comments made on social media, including Facebook, Twitter, Instagram & WhatsApp regarding Downe House Riyadh will be taken seriously and investigated thoroughly by our ICT manager, and any parent/s thought to be involved in the incident will be asked to attend a meeting with the Principal and member of the school governing body. In extreme cases parents may be asked to withdraw their child / children from the school.

I have read the acceptable use agreement for devices and social media and agree to follow the above document in order to support the integrity and safe use of ICT at Downe House Riyadh .

Child's name:_____ Class:_____

Parent signature:_____ Date:_____

Downe House
Riyadh

ICT ACCEPTABLE USE AGREEMENT – PRE-PREP

(PARENTS TO SIGN)

Please read and discuss the e-Safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation, please contact the school.

Downe House Riyadh Pupil ICT Acceptable Use Agreement / e-Safety Rules

- I will only use ICT in school when my teacher tells me to.
- I will not tell other people my passwords.
- I will only open my own work.
- I will make sure that all messages with other children and adults are polite and sensible and I will only use kind words.
- If I accidentally find anything on the internet that upsets me I will tell my teacher immediately.
- I will not talk to strangers on the computer.
- I will use gentle hands when using computers.

We have discussed the above and.....(child name) in class ….....agrees to follow the e-Safety rules and to support the safe use of ICT at King's College Doha.

Parent: _____

Date: _____

Downe House
Riyadh

ICT ACCEPTABLE USE AGREEMENT – PREP & SENIOR SCHOOLS

(PUPILS TO SIGN)

- I will only use ICT in school for school purposes.
- I will only use the school email software when conducting school related activities.
- I will only open email attachments from people I know, or who my teacher has approved.
- I will not tell other people my ICT passwords.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant, offensive or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out my own details online or via messages such as my name, phone number or home address. I will not arrange to meet someone.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I know that my use of ICT can be checked and that my parent/ carer can be contacted if a member of the school staff is concerned about my e-Safety.
- I understand that there will be consequences should I break any of the e-Safety rules.

Stay Safe

Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never agree to meet up with someone you have met online, this can be very dangerous. Only meet up if you have first told your parent or carer and they agree to attend the meeting with you. Remember that information online can be untrue, biased or just inaccurate. Someone online my not be telling the truth about who they are - they may not be a 'friend'.

Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something you have seen online or if someone you don't know has contacted you online. Emails, downloads, instant messages, photos and anything from someone you do not know, or trust may contain

a virus or unpleasant message. So do not open or reply.

Name of Child: _____

Class: _____

Parent: _____

Date: _____

Downe House
Riyadh

ICT ACCEPTABLE USE AGREEMENT – STAFF

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This agreement is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this agreement and always adhere to its contents. Any concerns or clarification should be discussed with the ICT manager or Principal. Deliberate access to inappropriate materials by any user will lead to the incident being logged by the ICT manager and depending on the seriousness of the offence, investigation by the Principal. In serious cases, immediate suspension, possibly leading to dismissal could take place. Local authorities may also be contacted if deemed necessary.

- I will only use the school's email / internet / intranet / website and any related technologies for professional purposes or for uses deemed 'reasonable' by the Principal.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils or parents.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on Pupil Asset) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Principal.
- I will not install any hardware or software without seeking permission from the Principal and ICT manager.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal, or discriminatory. Images of pupils and/ or staff will only be taken, stored, and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to the ICT manager and Principal.
- I will respect copyright and intellectual property rights. Upon leaving the school I will not corrupt, delete or remove any documents or files.

- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature:

I agree to support the safe use of ICT throughout the school and comply with the terms of this agreement.

Signature: _____

Date: _____

Full Name: _____(printed)

Job title: _____