ICT AND USE OF THE INTERNET AND INTRANET BY PUPILS

Reviewed without change: August 2025
Next review: August 2026

Status: non-statutory.

This policy should be read in conjunction with the following policies:

- Pupil behaviour.
- E-safety.
- Social media.
- Safeguarding and Child protection.

Background

Information and Communications Technology (ICT) is vital for preparing pupils for a rapidly changing world where many activities are transformed by evolving technology. It serves as a fundamental tool in the teaching and learning process, enabling pupils to find, process, and responsibly use information. All staff and pupils need to become confident users of ICT so that they can develop the skills, knowledge and understanding which enables them to use appropriate ICT resources effectively as powerful tools for teaching and learning.

Governors are responsible for ensuring the school's ICT resources have appropriate filters and monitoring systems in place. They also are required to ensure that staff undergo regular safeguarding training, including online safety training, and that pupils are taught about e-safety, for example through personal, social, health and economic education (PSHE).

The internet offers children and young people a wealth of opportunities for entertainment, communication and education. However, it also poses risks, including exposure to inappropriate content and the potential for harm due to the deliberate actions of others online. Under the prevent duty in particular, there is a legal requirement for schools to have due regard to the need to prevent individuals being drawn into terrorism.

ICT AND USE OF THE INTERNET AND INTRANET BY PUPILS

AT DAR UL MADINAH SCHOOL ALL OUR SYSTEMS ARE CLOSELY MONITORED

Introduction

This policy governs the use of ICT facilities by pupils at Dar ul Madinah School. A separate policy governs staff usage.

The internet offers children and young people a wealth of opportunities for entertainment, communication and education. However, it also poses risks, including exposure to inappropriate content and the potential for harm due to the deliberate actions of others online. Pupils at primary school learn the principles for keeping safe online and this is developed at secondary school where they learn about the opportunities offered by the internet as well as the risks and their own responsibilities when working online.

Dar ul Madinah School has procedures in place to safeguard all learners from unlawful, sexual or otherwise potentially harmful content on the internet. Information on internet safety and the importance of monitoring internet use at home is made available to all parents annually.

There are many computers available for use by pupils and the majority of these have access to the internet through the school network. All pupils have a login name, password and an email account. The email system is available for use both from within the school and externally using a web browser. There are specialist centres serving design, mathematics and science departments together with general purpose rooms. A growing number of other computers are located within individual departments/classroom areas.

Objectives and targets

The objective of this policy is to develop an appropriate code of practice for use of ICT by pupils at Dar ul Madinah School.

Action plan

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that:

- Pupils can only access data to which they have right of access.
- No pupil should be able to access another’s files without permission.
- Access to personal data is securely controlled in line with the school’s Internal data security policy and as required by the General Data Protection Regulation (GDPR).
- Logs are maintained of access by pupils and of their actions while users of the system.

All pupils are expected to sign the ICT: Pupil acceptable usage agreement (see appendix 1) and all visiting pupils are expected to sign the ICT: Visiting pupil acceptable usage agreement (see appendix 2).

Rights of access – pupils
A safe and secure username/password system is essential and will apply to all school ICT systems, including email and virtual learning environment (VLE).

All passwords are generated by the network manager/ICT technical support staff and are unique to each pupil. Passwords can only be reset by the user or by the ICT technical team. All pupils will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the network manager and these will be reviewed, at least annually. The 'master/administrator' passwords for the school ICT system used by the network manager/ICT technical support team are also available to the headteacher or other nominated senior leaders and kept in a secure place (eg school safe). In the event of a serious security incident, the police may request, and will be allowed access to, passwords used for encryption.

ICT code of practice – pupils
The following code of practice must be adhered to by all pupils.

- The facilities are provided to support and enhance curriculum-related activities. Each pupil will be issued with his/her own username and password, which must be kept confidential. Pupils must remember to log off when they have finished using the computer. It is good practice to change passwords regularly.

- The pupil's school email address must always be used for all school-related activity. Personal emails must not be used for any school-based activity.

- The use of another person's user name and password, abusive language, sending abusive messages and changing computer settings are all serious offences.

- Pupils must not copy, alter, print or change another pupil's work in any shape or form without the person's prior knowledge and consent. Please note that copyright regulations apply to electronic publications as they do to paper.

- Pupils must use the internet and printing facilities only to support their school work.

- Pupils should be aware that information on the internet may not always be reliable and sources should be checked. Also websites are used for advertising material, which may influence the contents.

- Emails are not confidential and do go astray. Therefore we must guard against any abuse which will bring the school into disrepute.

- Pupils must not disclose to anyone on the internet their home address, telephone number, the name of the school or a photograph of themselves unless specific permission is given from a member of staff. Nor should they ever arrange to meet anyone unless this is part of a school project approved by their teacher.

- Pupils must never pretend to be anything or anyone that they are not and must be aware that the posting of anonymous messages is forbidden.

- Pupils must not engage with internet chatrooms.

- Pupils must not engage with any organisations over the internet which could be considered to support extremism, radicalisation or terrorism of any kind.

- If a pupil sees something which makes her/him feel worried or uncomfortable, s/he should report it immediately to a member of staff and never respond to bullying, suggestive or unpleasant emails or blog entries.

- Pupils must not send abusive email, chain email, excessive quantities or excessive sized emails. Nor must they use email to send or encourage material that is pornographic, illegal, offensive or invades another's privacy.

- Pupils must not vandalise the system by:

    - Physical damage.

    - Changing configuration or cabling unless specifically directed by a member of staff.

    - Hacking of the school or external systems. Pupils should be aware that hacking into computers is a criminal offence and they could be prosecuted under the Computer Misuse Act 1990.

    - Changing the contents of the hard disks.

    - Downloading or installing software onto the network, unless written as part of an approved school computer project and with the teacher's permission.

    - Bringing food and drink into computer areas or in the vicinity of classroom computers because spillages can cause serious damage to electronic equipment.

Misuse of computer systems by pupils

Internet and email

Please note that in the case of misuse of internet and email facilities the following action will be taken:

- **First offence** – the pupil will be reported to the network manager and will have access to the internet and email withdrawn for two weeks. Parents will be informed. The pupil will still have access to intranet and basic application software.

- **Second offence** – procedure as above but with a four week ban and a formal letter sent home to parents.

- **Third offence** – parents will be invited to a formal meeting with the e-safety member of the senior leadership team, to discuss the way forward and sanctions.

Pupils who use other pupils' accounts and access restricted file areas

These are considered to be serious offences. The network manager will record the offence and will immediately inform the year tutor of the situation. Suspension of a pupil's access to all ICT facilities will take place after the year tutor has informed the appropriate staff.

The length of the ban may vary according to circumstances but it is likely to be for at least four weeks.

To restore access, a note is required from the year tutor.

Damage to hardware

If a pupil damages hardware, the network manager will contact the main office staff. A letter will be sent to parents. The pupil will be charged for the damage.

Accessing websites which could be considered to support extremism, radicalisation or terrorism
If a pupil is found to engage over the internet with any organisations which could be considered to support extremism, radicalisation or terrorism of any kind then the matter will be reported to the headteacher who has a legal obligation to report it to the local authority (LA).

Other serious offences and inappropriate use of ICT facilities
Other serious offences and inappropriate use of ICT facilities will result in the following sanctions:

- An immediate ban from the network pending investigation.
- A letter home informing parents of incorrect ICT use and a minimum ban of two weeks from the internet/email facilities.
- Subsequent offences will lead to a four to eight week ban and/or an exclusion of three days from school.
- More serious or long term abuse will lead to a total network ban and possible exclusion from school.

Under exceptional circumstances, such as abuse which may be detrimental to the school network, the network manager may disable a pupil's account with immediate effect.

Monitoring and evaluation

The policy will be monitored and evaluated regularly taking into account any incidents which occur or technological developments which might need a change in the policy.

Reviewing

The efficacy of the policy will be discussed annually as part of the governors' rolling programme of reviews.

APPENDIX 1

ICT: Pupil acceptable computer usage agreement

(This agreement could usefully form part of any agreement/permissions pack provided for any new entrants to the school. Two copies should be signed – one to be returned to school for the pupil file and the other retained by pupil/parents for reference.

Guideline for all users of the school network

Access to the school network and internet is provided for you to carry out recognised schoolwork. This provision will only be made on the understanding that you agree to follow these guidelines:

- Computer (file) storage areas are treated as school property. ICT staff may look at files and communications to ensure that the system is being used responsibly. I do not expect my work and emails to be private
- I am aware that a member of the ICT staff could view my computer screen, from the school network, without my knowledge, at any time.
- I understand that I am responsible for good behaviour and that general school rules apply while using the computers.
- I understand that eating, drinking, personal grooming or the use of aerosol sprays near a computer may cause serious damage and are strictly prohibited.
- I will not reveal my password to anyone. If I think someone knows my password, then I will change it.
- I will not use another person's password. If I am doing shared work I will email a copy to my own work area.
- I understand that programs must not be loaded or installed on a computer except by ICT support staff.
- I will not bring programs in on removable media, email or download them from the internet.
- I understand that the use of the internet is a privilege and provided for pupils to conduct genuine research and communicate with others.
- I understand that all the internet sites that I visit are recorded.
- I understand that I must not download any files without permission.
- I understand that I must not use messaging apps (eg WhatsApp, Facebook messenger).
- I understand that I must not use chat, play games, use mobile ring tones sites or SMS sites.
- I understand that I must not use web mail (eg Hotmail, Gmail, Yahoo), other than that provided for my school account.
- I understand that I must not use obscene or offensive language. I will remember that communication should be polite to maintain the good reputation of the school.

- I understand that I must not seek out any organisations over the internet which could be considered to support extremism, radicalisation or terrorism of any kind.
- I understand that I must not seek out any offensive material.
- I understand that I must not complete mailing lists or subscription forms on the internet for personal use.
- I understand that I must not violate copyright laws. (Never copy and make use of any material without giving credit to the author. Copyright, Designs & Patents Act 1988). If I am unsure then I will ask a member of staff for advice.
- I understand that I must not attempt hacking into the computer systems of the school or any other organisation. (I am aware that hacking into computers is a criminal offence and I could be prosecuted under the Computer Misuse Act 1990).

Sanctions

- I understand that violations of the above rules will result in sanctions being taken. (These sanctions are outlined in the school's policy on ICT and use of the internet and intranet by pupils).
- I understand that I am always subjected to the Data Protection Act, the General Data Protection Regulation, Computer Misuse Act 1990 and Copyright, Designs and Patents Act 1988.

The School reserves the right to seek remuneration from parents of pupils who cause malicious damage to ICT equipment.

During lessons, teachers will guide pupils toward appropriate materials. However, outside lessons, families bear this responsibility.

Please sign both copies - return one copy to the school and retain the second copy for your records.

We agree to the terms and conditions of the ICT: Pupil acceptable computer usage agreement.

Name of pupil: …….. Tutor group: ……..……

Pupil's signature: …… Date: ……

Parent/Carer's signature: …… Date: ……...

APPENDIX 2

ICT: Visiting pupil acceptable computer usage agreement

As a visitor to Dar ul Madinah School we ask you to act sensibly and properly at all times and accept the guidelines for visitors who use the school network. Access to the school network and internet is provided for you to carry out recognised schoolwork. This provision will only be made on the understanding that you agree to follow these guidelines.

- Computer (file) storage areas are treated as school property. ICT staff may look at files and communications to ensure that the system is being used responsibly. I do not expect my work and emails to be private
- I am aware that a member of the ICT staff could view my computer screen, from the school network, without my knowledge, at any time.
- I will not reveal my password to anyone. If I think someone knows my password, then I will change it.
- I will not use another person's password. If I am doing shared work I will email a copy to my friend.
- I understand that programs must not be loaded or installed on a computer except by ICT support staff.
- I will not bring programs in on removable media, email or download them from the internet.
- I understand that all the internet sites that I visit are recorded.
- I understand that I must not seek out any organisations over the internet which could be considered to support extremism, radicalisation or terrorism of any kind.
- I understand that if I find inappropriate material I will advise the teacher immediately.
- I understand that I am always subjected to the Data Protection Act, the General Data Protection Regulation, Computer Misuse Act 1990 and Copyright, Designs and Patents Act 1988.
- I understand that I must not attempt hacking into the computer systems of the school or any other organisation. (I am aware that hacking into computers is a criminal offence and I could be prosecuted under the Computer Misuse Act 1990).

Sanctions

- If you cannot act sensibly and properly your teacher will remove you from the computers and further sanctions may be taken. (These sanctions are outlined in the school's policy on ICT and use of the internet and intranet by pupils).

The school reserves the right to seek remuneration from parents of pupils who cause malicious damage to ICT equipment.

Please sign and return to your teacher

I agree to the terms and conditions of Dar ul Madinah School ICT: Visiting pupil acceptable computer usage agreement.

Name of pupil: …….. Tutor group: ……..……

Pupil's signature: …… Date: …….