DARUL ULOOM

E-SAFETY POLICY

September 2024

Ratified by the Trustee: 30 August 2024
Signed by the Trustee: 30 August 2024

To be reviewed: 01 September 2025

This policy should be read in conjunction with:
1. Safeguarding policy 2. GDPR policy 3. Behaviour policy 4. Anti-bullying policy 5. Staff Code of Conduct 6. KCSIE September 2024

Contents

"And keep yourself (O Muhammad!) patiently with those who call on their Lord (your companions who remember their Lord with glorification, praising in prayers, etc., and other righteous deeds, etc.) morning and afternoon, seeking His Face, and let not your eyes overlook them, desiring the pomp and glitter the life of the world; and obey not him whose heart We have made heedless of Our Remembrance, one who follows his own lusts and whose affair (deeds) has been lost." The Holy Quran: 18:28.

Introduction
ICT in the 21st Century is seen as an essential resource to support learning and teaching and plays an important role in the everyday lives of children, young people, and adults. Consequently, schools must incorporate these technologies to arm our young people with the skills to access life-long learning and employment.

Information and Communication Technology covers various resources, including web-based and mobile learning. Recognising ICT's constant and fast-paced evolution within our society is also essential. Currently, the internet technologies children and young people are using both inside and outside of the classroom include:
- Websites
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs, Wikis and Tweeters
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- iPads
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, is not consistently policed. All users must be aware of the risks of using these internet technologies.

At *Darul Uloom***, we understand the responsibility to educate our pupils on e-safety issues,** teaching them the appropriate behaviours and critical thinking skills to remain safe and legal when using the internet and related technologies in and beyond the classroom context. To support them further and ensure their safety whilst using technology, the school has taken the initiative to ensure filters are in place to block all inappropriate, sensitive, and incriminating websites. The School uses Impero to monitor the use of computers and the Internet.

Purpose
This policy defines and describes the acceptable use of IT for staff and students at Darul Uloom. Its purpose is to encourage the creative use of technology to engage learners, minimise the risks to students of inappropriate situations and materials, protect the staff and school from litigation and minimise the risk to the IT network and systems.

This policy governs the use of IT facilities and associated web-based services across the School and applies to all school employees, students, and authorised users.

Roles and Responsibilities

- The trustees are responsible for ensuring that its employees act lawfully and appropriately use school technologies for approved purposes only.

- The Headteacher is responsible for implementing relevant policies and ensuring staff know their contents.

- The School Headteacher is responsible for maintaining an IT equipment inventory as part of the school asset management register and recording to whom it has been issued.
- If the School Headteacher believes that an adult has misused any IT equipment, he will consult the Trustee for advice without delay. The Trustee will agree with the School Headteacher an appropriate strategy for investigating the allegations and liaison with other agencies as appropriate. Incidents will be investigated

promptly by agreed procedures. The School Headteacher will clarify that internal school staff should not conduct any investigations unless they are both qualified and authorised. *It is also important to recognise that e-safety is not an IT issue. It may involve IT, but it is about protecting children and young people from harm. If you are concerned about actual, significant harm to a child or young person or the risk of significant harm, you should immediately contact the Designated Safeguarding Lead (DSL) in the school.*

IT User Responsibilities

- Use of the school's IT resources is granted based on acceptance of the followingspecific responsibilities:
- Use only the computing and information technology resources you have authorised. To agree to the terms and conditions of use when signing in to the P.Cs.

    For example, it is a violation
- to use resources, you have not been specifically authorised to use
- to use someone else's account and password or share your account andpassword with someone else
- to access files, data or processes without authorisation
- to purposely look for or exploit security flaws to gain system or data access
- Use computing and information technology resources only for their intended purpose.

    For example, it is a violation
- to send forged email or other electronic communication
- to misuse Internet software to allow users to hide their identity or to interfere with other systems or users
- to use electronic resources for harassment or stalking other individuals
- to send chain letters, bomb threats or "hoax messages"
- to intercept or monitor any network communications not intended for you
- to use computing or network resources for advertising or other commercialpurposes
- to use electronic resources for personal use at inappropriate times or ininappropriate locations
- to attempt to circumvent security mechanisms
- Protect the access and integrity of computing and information technologyresources.

    For example, it is a violation
- To intentionally release any malware that damages or harmsa system or network
- to prevent others from accessing an authorised service
- to send email bombs that may cause problems and disrupt service for other users
- to attempt to degrade performance or deny service deliberately
- to corrupt or misuse information
- to alter or destroy information without authorisation
- Abide by applicable laws and school policies and respect the copyrights andintellectual property rights of others, including the legal use of copyrighted software.

    For example, it is a violation
- to make unauthorised copies of licensed software
- to download, use or distribute pirated software
- to upload or download pirated copies of video or audio files
- to operate or participate in pyramid schemes
- to upload, download or distribute inappropriate material
- Respect the privacy and personal rights of others.

    For example, it is a violation
- to tap a phone line or run a network sniffer without authorisation
- to use photographs of individuals for School purposes withoutpermission
- to access or attempt to access another individual's password or data without explicit authorisation from a senior staff member, with the School Headteacher's direct knowledge.

Reporting

Staff are responsible for reporting every breach of e-safety. If a staff member knows or suspects that a colleague is in breach of any part of this policy, he/she must report it to the appropriate person in writing by email to the following leads and copy the School Headteacher.

Immediate reporting:

- Safeguarding incident to DSL
- Inappropriate activity by a member of staff to the SLT
- Illegal content or material which requires immediate removal or blocking to SLT and ICT lead
- Inappropriate material which requiresadditional filtering on the Internet to SLT and ICT lead
- Inappropriate activity by a student in a lesson (which does not constitute a safeguarding incident) to the SLT and ICT lead
- Inappropriate activity by a student not in a lesson (which does notconstitute a safeguarding incident) to the SLT and ICT lead

Staff are required to be vigilant when students are using computers. Students accessing inappropriate materials must be reprimanded, and repeated offences must be reported using the school's behaviour systems.

Acceptable and Unacceptable Use

- Rapid developments in hardware and software mean that technology use changes at an unprecedented rate. Documenting every potential use of IT equipment in school would be impossible.
- Within the school, we believe technology is an essential part of education in the 21st century. Young people are immersed in a digital world where information is available 24 hours a day, 7 days a week. The Internet and other digital and information technologies are powerful tools that open up new opportunities for everyone. These technologies can encourage discussion, provide outlets for creativity and enrich the curriculum. The use of e-mail, mobile phones, Internet messaging and blogs all enable improved communication on an unprecedented scale. Our Virtual Learning Environment will offer a platform for personalised and independent learning.
- In addition to these benefits, however, there are risks, and unfortunately, some young people may expose themselves to danger either knowingly or unknowingly.
- Staff and students may inadvertently encounter unsavoury, distressing, or offensive materials on the Internet, and some social networking sites offer cover for unscrupulous individuals to groom children. It is crucial that while promoting the positive use of technology in our school, we recognise the potential risks and take steps to protect our students, staff, and visitors.
- Instead, the incorrect use of IT within the school is underpinned by the term 'Unacceptable Use'.
- Unacceptable Use is defined as any activity conducted without permission, outside the specific learning aim for that lesson or activity, illegal, considered extreme or radicalising, dangerous, or where the equipment is used to make any student, member of staff, or member of the public feel uncomfortable or vulnerable.
- Therefore, acceptable use means using the resources to create imaginative learning, efficient business practice, continuing professional development, and other uses that enable staff to maintain a healthy work-life balance.

Equipment and Services Summary

- *IT Equipment*—This term refers to any equipment provided by the school, including computers, portable devices, and phones.
- Any equipment must be used carefully, and precautions must be taken to ensure it is left ready for other userswhen finished. Damaged, broken or missing equipment must be reported immediately to the relevant person.
- *Network Login and Password*—All users are issued a username and password with access rights tailored for their use of the school's IT systems, provided they accept the responsibilities outlined in Appendix 2.
- All users must access the network only using their login and password. Passwords must not be disclosed

or shared. The user assumes full responsibility for the use or misuse of this account.

- *Personal Use*—Staff are permitted to use school IT equipment for personal use, provided it does not breach the term 'Unacceptable Use'. All users must use any equipment appropriately and responsibly at all times and assume full responsibility for any activity carried out using their account or on equipment being used by them at the time.

- *Internet Access* – A filtered and managed connection to the Internet is provided to all users. Staff and students must not access or attempt to access websites that contain any of the following: child abuse, pornography, extreme or radicalising views, promotion of discrimination of any kind, promoting illegal acts, or any other information which may be illegal or offensive. It is recognised that under certain circumstances, inadvertent access may occur. Should staff or a student access any sites which may fall into the categories described above you must report it by the reporting procedures.

- *Email*—Each staff member and student is provided with an email account. All communications for professional business, including contact with students and parents, must be done through the school email systems. Any emails sent through the school system must be appropriate and professional.

- *Monitoring* – Internet activity, network activity and email are subject to monitoring and may be viewed without prior warning.

- *Images and Videos* – We encourage staff and students to use IT to capture work and achievements as part of a portfolio of evidence or to celebrate work or accomplishments. No images or videos should be uploaded to any website or social network without permission and in the case of students, this includes the permission of the parents/carers. No images or videos of students should ever be uploaded to staff personal websites or social network accounts. For images and videos with visitors, please see the visitor policy

- *Copyright, including Software licensing*—*The school provides all users with access to a range of software and services licensed by agreements with the companies involved. Only licensed copies of software may be installed on any device. Users may not download copyrighted software, audio or video files,* or any other copyrighted material. Any such material found will be deleted without prior notification.

- *Data Protection* – A large amount of personal and sensitive data is held on the school systems regarding students, staff and trustees. All adults will take reasonable measures to ensure that no data is disclosed accidentally or deliberately. No copies of data regarding personnel or students will be retained on any personal device including a home computer, USB stick, or any other portable storage. When working on school data remotely, including at home, every effort will be made to ensure it is not disclosed to or accessed by anyone else.

- *Bring Your Device* – Staff are permitted to use their own personal IT equipment in school at the discretion of the School Headteacher. The use of any personal device on school grounds or if being used for a work-related activity is subject to the same principles of 'unacceptable' use as any device owned by the school. The member of staff is responsible for ensuring that any device brought into school by them is used appropriately and within the scope of this policy. The staff member is responsible for any use or misuse of this device while on school grounds or if it is being used for a work-related activity. You are responsible for ensuring that any use follows the Data Protection procedures outlined.

Safer Social Networking Practice

- This section applies to current social networking sites such as Facebook, Tumblr, LinkedIn, Twitter, Snapchat, Instagram and all other current and emerging technologies.

- All adults must adhere to, and apply the principles of this document in all aspects of their work. Failure to do so may lead to action being taken under the disciplinary procedure.

- In their interests, adults in school settings must be aware of the dangers of putting their personal information onto social networking sites, such as addresses, home or mobile phone numbers. This will avoid the potential for students or their families or friends having access to staff outside of the school environment. It also reduces the potential for identity theft by third parties.

- All adults, particularly those new to the school setting, should review their social networking sites when they join the school to ensure that information available publicly about them is accurate and appropriate. This includes any photographs or posts that may cause embarrassment to themselves and/or the school if they were to be published outside of the site.

- As security settings change frequently, all staff are encouraged to regularly check that accounts remain secure.

- Adults should never befriend, follow, contact or link with a student at the school where they are working

on any personal social networking page, and should be extremely cautious about links with ex-students particularly where siblings or other relatives maycontinue to attend the school.

- Friend/contact requests from any student on roll at the time must be declined and reported to the SLT.
- Staff should never use or access social networking pages of students unless specifically directed to do so by the headteacher as part of an investigation
- Confidentiality must be considered at all times. Social networking sites have the potential to discuss inappropriate information and employees need to ensure that they do not put any confidential information on their site about, the school, the trustees, their colleagues, students or members of the public.
- Staff need to ensure that when they are communicating about others, even outside of work that they give due regard to the potential for defamation of character. Making allegations on social networking sites (even in their own time and in their own homes)about other employees, students or other individuals connected with the school, or another school could result in disciplinary action being taken against them.
- Adults within the school setting must never post derogatorily remarks or offensive comments online or engage in online activities which may bring the school into disrepute or that could be interpreted as reflecting negatively on theirprofessionalism.

Communications and Social Contact

- Adults should keep their personal phone numbers, work login or passwords andpersonal email addresses private and secure. Where there is a need to contact students or parents a school system should be used e.g., telephone, email or messaging service.
- Adults must understand who is allowed to view the content on their pages of any sitesthey use and how to restrict access to certain groups of people.
- Communication between students and adults by whatever method, must take placewithin clear and explicit professional boundaries. Staff should use their school emailfor all contact with students.
- Adults must not request, or respond to, any personal information from a student.
- Adults must ensure that all communications are transparent and open to scrutiny. They should also be circumspect in their communications with students in order to avoid any possible misinterpretation of their motives or any behaviour which could possibly be construed as 'grooming' in the context of sexual offending.
- E-mail or text communications between an adult and a student outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications through internet-based web sites. Internal e-mail systems must onlybe used in accordance with the school's policy.
- There may be occasions when there are social contacts between students and staff, where for example the parent and teacher are part of the same social circle. These contacts however, will be easily recognised and should be openly acknowledged with the Headteacher where there may be implications for the adult and their position withinthe school setting.
- There must be awareness on the part of those working with or in contact with students that some social networking contacts, especially where these are not common knowledge, can be misconstrued as being part of a grooming process. This can also apply to social networking contacts made through outside interests or through the adult's own family.
- Any concerns must be raised with the Headteacher at the earliest opportunity.

Access to Inappropriate Images

There are no circumstances that justify adults possessing indecent images of children. Staff who access and/or possess links to such material or websites will be viewed as asignificant and potential threat to children. This will lead to criminal investigation and disciplinary action. Where indecent images of children are found, the Headteacher must be informed immediately.

Adults must not use equipment belonging to the school to access any adult pornography or any inappropriate images; neither should personal equipment containing these images or links to them be brought into the workplace. This will raiseserious concerns about the suitability of the adult to continue to work with children.

Adults should ensure that students are not exposed to any inappropriate images or web links. The school endeavours to ensure that internet equipment used by students has the appropriate controls with regards to access. e.g. personal passwords should be kept confidential. Any potential issues identified must be reported to the ICT lead immediately.

Where other unsuitable material is found, which may not be illegal but which could or does raise concerns about a member of staff, advice should be sought from the ICT lead before any investigation is conducted.

Cyberbullying

- By adopting the recommended 'no use of social networking sites on school premises', Darul Uloom protects themselves from accusations of complicity in any cyber bullying through the provision of access. Parents should be clearly aware of the school's policy of access to social networking sites.
- Where a disclosure of bullying is made, schools now have the duty to investigate and protect, even where the bullying originates outside the school. Once disclosure is made, investigation will have to involve the families. This should be dealt with under the school's adopted anti bullying policy. If parents / guardians refuse to cooperate with our policy and bullying continues, it can be referred to the police as harassment. This guidance can also apply to text and mobile phone cyber bullying.
- Cyberbullying can be defined as 'the use of modern communication technologies to embarrass, humiliate, threaten or intimidate an individual in the attempt to gain power and control over them.'
- If cyberbullying does take place, employees should keep records of the abuse, text, e-mails, website or instant message and should not delete texts or e-mails. Staff are advised to take screen prints of messages or web pages and be careful to record the time, date and place of the site.
- Staff are encouraged to report any and all incidents of cyberbullying to the SLT or the Headteacher. All such incidents will be taken seriously and will be dealt with in consideration of the wishes of the person who has reported the incident. It is for the individual who is being bullied to decide whether they wish to report the actions to the police. Staff may wish to seek the support of their trade union or professional association representatives.

Data Protection, GDPR And External Software

All using ICT on the school premises and related to it are required to abide by the GDPR to ensure the safe usage of data, avoiding its breach of any manner. The school has employed the background software Link2ICT's *Futures Cloud* (formerly known as *Policy Central*) to monitor use of ICT, which effectively flags any concerning behaviour. The Data Protection Act 1998 (DPA), states that anyone processing personal data must comply with the eight enforceable principles of good practice. They say that data must be:

- fairly and lawfully processed
- processed for limited purposes
- adequate, relevant and not excessive
- accurate
- not kept longer than necessary
- processed in accordance with the data subject's rights
- secure
- Not transferred to countries without adequate protection

This applies to the School Personal data includes both facts and opinions about any living or identifiable individual. As an organisation we need to understand the roles of those involved in processing and storing data about students and the need to understand the concepts of 'obtaining', 'holding' and 'disclosing' information.

Copies of student reports form part of the student's educational record. We are required to compile a curricular record for each student, and it must be updated at least once a year. This is a formal record of academic achievements, other skills and abilities, and progress in school. Additional records may be kept - for example, a

detail of behaviour and family background - but this is not compulsory. This material, together with copies of a student's report, makes up the student's educational record. Any communications between the School Head Teacher and teachers at the school, other employees at the school or the Trustees, form part of a student's educational record. Communications from parents, another student or a member of the local community which refer to a student do not form part of that student's educational record.

Under the Data Protection Act, all students are entitled to request a copy of their educational records, free of charge, within 15 school days of making a written request. If a student seeks access to his records, the school should establish whether the student understands the nature of the request. If the school thinks the student does not understand owing to youth or immaturity, the request can be denied.

Parents can request a copy of their son's educational record. The request should be made in writing, and the school should supply the documentation within 15 school days, free of charge or at no greater cost than that of supplying it. Where a student asks for a copy of his educational record, any charge must be no higher than the cost of supply or the cost allowed under the Data Protection Act, whichever is the lesser.

All requests for educational records should be passed immediately to the Headteacher before actioning.

- Users must access the network only using their own logins and passwords. These must not be disclosed or shared.
- The user takes full responsibility for the use or misuse of this account.
- Staff must logout or lock of ET-AIMS, Gmail and their PC when leaving a classroom for any period of time.
- If a member of staff is made aware of any inaccuracy in the personal data of an individual, they must make the school office staff aware.
- Staff must take care not to accidentally disclose personal information via the interactive whiteboards in a classroom, or public view of a computer screen, including displaying ET-AIMS on a classroom whiteboard.
- Staff are responsible for removing material from IT systems which is no longer relevant.
- Any disclosure, whether deliberate or accidental must be reported to the Headteacher immediately.
- If a member of staff knows that a colleague is in breach of the Data Protection Act, he/she must report it to the Headteacher.
- If a member of staff suspects that a colleague is in breach of the Data Protection Act, they must seek clarification from the SLT and/or report it to the Headteacher.
- Personal data may only be taken off site by designated staff, for the completion of educational reports. However, no copy of the data may be left on any personal IT equipment (either in the School or at home). Whilst working at home, staff must take care not to accidentally disclose personal information to any third party.
- Personal data must not be transferred to any storage external to the School network or managed cloud services (including flash memory or personal cloud based-storage) unless it has been encrypted.
- Personal data may not be transferred outside the UK unless as part of a managed, organised move, co-ordinated by the Headteacher .
- Personal data may not be sent to any third party unless they are a designated organisation, covered by the School's entry in the Data Protection register.
- The school will record CCTV images on a secure, dedicated system.
- Staff who allow additional images to be recorded are advised to ask the person recording the image what the purpose is, where it will be stored and how it is to be manipulated. Where staff are concerned or unsure about the use of this image, they have the right to refuse permission for additional images to be recorded. Please see the visitor policy for further guidelines.
- If in doubt, seek clarification from your line manager, a member of SLT, the ICT lead or the Headteacher.

Use of the School Hardware and Network (via any wired or wireless device):

- Staff must sign the 'IT User Responsibilities' agreement before access to the network is permitted.

- Users shall not in any way, tamper or misuse school equipment, either software or hardware.
- Users must only access the network using their own logons and passwords. These must not be disclosed or shared.
- Users must respect confidentiality and attempts should not be made to access another individual's personal folder on the network without permission.
- The user takes full responsibility for the use or misuse of this account.
- Software, including apps should not be installed without proper licensing arrangements.
- Machines must never be left 'logged on' and unattended. If a machine is to be left for a short while, it must be 'locked.' (Ctrl+alt+del followed by 'lock computer').
- Machines must be 'logged off' correctly after use.
- Users must not make any attempt to remove, replace or disable the anti-virus software installed on any school device.
- Staff must logout of HUB when leaving a classroom for any period of time.
- Access to storage areas on the network is permitted on an individual needs basis and will be determined by the School Headteacher.
- Staff must only place material for professional or educational purposes on the shared areas of the network.
- Staff are responsible for removing material which is no longer relevant.
- Devices in school can have access to the Internet. Abuse of this access, in the form of access to pornographic sites is absolutely forbidden. Please note that access to certain pornographic sites may be in serious breach of the law (Child Trafficking and Pornography Act 1998). The school will fully co-operate with the relevant authorities in investigating and prosecuting any such illegal access.
- The ICT facilities are for school related educational use and personal use only. The ICT facilities are not available for use on external projects or for work or business activities not associated directly with courses or the school. ICT facilities may not be used for any form of personal financial gain. Exam marking is acceptable.
- The contents of all mailboxes, PCs, server shares, cloud storage areas and caches operated by the school, remain the property of the school. The status of these data stores is similar to that of letters posted to the school to a post holder (not marked as personal and private).
- Notwithstanding that every effort is made to ensure that home folders and e-mail are secure, the school does not in any way guarantee the security of this data.
- Food and drinks should be kept well away from ICT equipment.
- The user should take care when shutting down and closing the lids of laptops to ensure that nothing is left lying on top of the laptop surface. This may result in damage not covered by warranties, in which case the user will be liable for repair costs.
- The user should take care when moving any portable device, especially tablets. Devices should be securely fastened in their protective cases (where applicable) before moving.

Installing software

- Only licensed software may be installed onto school owned devices.
- Software in use in the school is licensed in a correct and legal manner. However (except where explicitly stated), it is not available to users for home usage. Users should make no attempt to copy licensed or copyrighted material from the school network.
- Teachers are not authorised to install unlicensed software on any device. If a member of staff requires special or non-standard software to be installed on any device, it must be licensed in a correct and legal manner. The member of staff will be responsible for supplying licenses, media, and any documentation on request if not purchased through the IT budgets.
- Users may not download copyrighted software, audio or video files, or any other copyrighted material from the Internet. Any such material found will be deleted without prior notification.
- Breach of these conditions may lead to disciplinary action.

Use of mobile phones and other mobile devices

The school recognizes that mobile phones and technology is part of the modern world we live in and is to some

an essential facet of their lives. Parents use it to keep in touch with their children and the school takes no issue on such matters. However, with regards to the learning environment, mobile phones can severely disrupt the education of other students. In our experience we have found that pupils use mobile phones in secrecy access social networking sites, take unauthorized pictures of other pupils and generally misuse them during school. Therefore, with great consideration, we have taken the preventative measure of banning mobile phones on school premises and requesting that they do not own one even at home.

Any parent wishing to communicate with their child should do so via reception bearing in mind that reception due to their own responsibilities, may not always be able communicate their messages to their child immediately.

If it is absolutely necessary for the child to carry a phone to and from school, it must be given in to the reception at the beginning of the day, and collected from the reception at the end of the day. The receptionist will keep their mobile phones secure in a safe. The school accepts no responsibility for loss or theft if correct procedures are not taken up. Therefore, we recommend students not to bring in a smart phone but a simple phone which is able to make calls and texts only.

If a pupil is found in possession of a mobile phone it will automatically be confiscated until the end of the term and parents will need to come in to collect it personally.

- If a pupil is late or enters school after form time, then they must submit their mobile phone to the reception and they can collect it at the end of the day. If they have to leave early for any reason, they should inform the office admin who will make arrangements for the phone's collection.
- The school reserves the right to search pupils for anything which has been banned, including a mobile phone. This policy is non-negotiable.
- Staff are required to switch mobile phones to silent during lessons, assemblies and other school based events.
- The taking of still pictures or video footage without the subject's permission is not ethical, and staff must ensure that any images captured for educational purposes are treated in accordance with the rules set out in the section referring to cameras.
- Any person recording any image for malicious purposes will be subject to disciplinary procedures.
- Students and staff are encouraged to report malicious texts or phone calls to the appropriate authority (including teaching staff)
- Staff are discouraged in their use of a personal mobile phone to access the Internet during school time and on school property as this by-passes the security systems set in place to protect individuals.
- For the use of mobile devices in relation to visitors, please refer to the visitor policy.

Use of Personal ICT equipment in School

- Staff must not bring any item of equipment onto the school premises which contains materials which directly contravene the e-safety policy. This may include e.g. inappropriate photographs or illegal copies of software.
- Any item which requires mains power, and which will be plugged into the school's electricity supply, must be Portal Appliance Tested (PAT) prior to use.
- Staff may connect their own devices to the wireless network in school. All access to the Internet must be conducted using their own login and password and all Internet traffic is subject to filtering and monitoring.

Use of the Internet and e-mail:

- Staff must sign the 'IT User Responsibilities' agreements before access to the internet and email is permitted.
- Staff may only send e-mails to students using the school e-mail system.
- Staff must not open e-mails sent from a current student's personal e-mail account unless there is specific permission from the school headteacher e.g. in the case of exams officers sending results to students.
- If a member of staff is sent an email by an ex student, they should only use the school e-mail system to respond.
- Users must access the Internet and e-mail using their own logon / password and not those of another individual. Passwords must remain confidential and no attempt should be made to access another user's e-mail account.
- The Internet and e-mail should primarily be used for professional and educational purposes. Personal use of the Internet is permitted provided it does not breach the term 'Unacceptable Use', does not contravene any other policy of the Trust or school and is carried out at appropriate times. Personal use of the Internet at inappropriate times or that breaches any other school or Trust policies may be subject to disciplinary procedures.
- All users must respect the need for Internet filtering and not deliberately try to by-pass the security systems.
- Students must be supervised at all times when using the Internet and e-mail in a learning situation.
- Accidental access to inappropriate, extreme or radicalising, abusive or racist material must be reported without delay to the ICT lead and a note of the offending website address (URL) taken so that it can be blocked.
- Internet and email filtering software is installed to restrict access, as far as possible, to inappropriate or offensive content and to reduce the receipt of 'spam,' junk or unwanted correspondence.
- Internet and email use will be monitored regularly in accordance with the Data Protection Act.
- All Internet account histories and school e-mail accounts are accessible to the ITManager and may be checked without prior consultation.
- Users must not disclose any information of a personal nature in an e-mail or on the Internet. This includes mobile and home phone numbers, addresses, or anything else which might allow them to be identified.
- All emails sent should be courteous and the formality and tone of the language used appropriate to the reader. No strong or racist language will be tolerated. Usage of any form of profanity in these communications is absolutely forbidden. Sanctions, appropriate to the case, will be imposed on any users who break this code.
- All emails sent from an establishment/service email account will carry a standard disclaimer disassociating the establishment/service with the views expressed therein.
- Bullying, harassment or abuse of any kind via e-mail will not be tolerated. Sanctions, appropriate to the case, will be imposed on any users who break this code.
- If users are bullied, or offensive emails are received, this must be reported immediatelyto a trusted adult or member of staff within the service / establishment. E-mails receivedshould not be deleted, but kept for investigation purposes.
- Anti-virus software is used on all machines and this is regularly updated to ensure its effectiveness.
- All users will be made aware of Copyright law and will acknowledge the source of any text, information or images copied from the Internet.
- E-mail should be considered as an insecure medium for the transmission of confidential information. Where confidential information is to be transferred, in particular externally,it should be done in an encrypted form.

Use of Chat and Weblogs during lessons

- Use of social-networking websites (e.g. Facebook, Twitter, Snapchat etc.) is not permitted during lessons unless the site is being accessed to make a specific educational point.
- Students and staff must not access public or unregulated chat rooms.

Use of Social Networking Sites

- Social networking sites are blocked

- Staff using such sites outside of school should not add current students as friends or contacts or use the site to contact current students. If staff do already have students as contacts, they are advised to delete these contacts with immediate effect.
- Staff are discouraged from adding ex-students as contacts as many of them have current students as friends and information can be disclosed to current students through these links.
- Staff should not put photographs of current students on any social networking site.
- Staff should ask for permission before putting photographs of other staff on any social media sites.
- Staff are advised not to add personal details to their social network sites for their own safety.
- Staff must not put personal details of their colleagues or students on their social network sites.
- Professional social media accounts are permitted providing the user follows the guidelines in the section headed 'Safer Social Networking Practice'

Use of Cameras, Video Equipment and Webcams

- All parents are notified of the school's policy on its use of student photographs and other media. A record of any response is kept up to date in the ET-AIMS.
- Photographs or video footage must be downloaded immediately and saved into a designated folder.
- Any photographs or video footage stored must be deleted immediately once no longer needed.
- Any adult using their own camera, video recorder or camera phone during a trip or visit must transfer and save images and video footage into a folder in a staff shared area of the network, at the earliest opportunity and delete the images from their own device.
- Students should not accept files sent via Bluetooth to their mobile phones by an unknown individual. If they do, and the content received is upsetting or makes them feel uncomfortable, they should pass this on to a trusted adult straightaway.
- Video conferencing equipment and webcams must be switched off (disconnected) when not in use.
- Webcams must not be used for personal communication and should only be used by students with an adult present and with written consent from parents / carers.
- Students and staff must conduct themselves in a polite and respectful manner when representing the establishment/service in a video conference or when corresponding via a webcam. The tone and formality of the language used must be appropriate to the audience and situation.

Safety of the school's website

- The school has a designated member of staff who is responsible for approving all content and images to be uploaded onto its website prior to it being published.
- The school website is subject to frequent checks to ensure that no material has been inadvertently posted, which might put students or staff at risk.
- Copyright and intellectual property rights must be respected.
- Permission will be sought from parents or carers before any images of students can be uploaded onto the school website.
- Full names must not be used to identify students portrayed in images uploaded onto the school website.
- When photographs to be used on the website are saved, names of individuals should not be used as file names.
- Any part of the school website which contains a Guestbook, public noticeboard, forums or weblogs, will be monitored regularly to check that no personal information or inappropriate or offensive material has been posted.
- Using portable games consoles and media players
- The use of portable games consoles and media players for students is only permitted at social times, unless specifically directed by a member of the teaching staff during a particular educational activity.
- Staff are encouraged to take a professional attitude in their own use of portable games consoles and media players in school time.
- Staff must not arrange to contact current students via online gaming forums and must refuse invitations from current students.

E-Safety in the Curriculum

- The school has a framework for teaching internet and communications skills in ICT & computing lessons.
- The school provides opportunities within a range of curriculum areas to teach about e-Safety.
- Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the e-Safety guidance linked to the curriculum .
- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities.
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline/ CEOP report abuse button.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.

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
- 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, e.g. 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 where consent could be an issue, e.g. divorce of parents, custody issues, etc. Parents/ guardians may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid. Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published. Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed. Only the Web Manager has authority to upload to the site.

Storage of Images
- Images/ films of students are stored on the school's network.
- Rights of access to this material are restricted accordingly to delegated staff members

Additional points to consider
- Participants in conferences offered by 3rd party organisations may not be DBS checked.

- Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference.

Equal Opportunities Pupils with additional needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the school's e-Safety rules. However, 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. Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-Safety. Internet activities are planned and well managed for these children and young people.

Parental Involvement

- Parents / careers and pupils are actively encouraged to contribute to adjustments or reviews of the school e-Safety policy in writing.
- Parents / careers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school.
- Parents / careers are required to make a decision as to whether they consent to images of their child being taken / used in the public domain (e.g., on school website)

The school disseminates information to parents relating to e-Safety where appropriate in the form of:

- Information and celebration evenings
- Posters
- Website/ Learning Platform postings
- Newsletter items