KD GRAMMAR SCHOOL FOR BOYS

FAITH • LEARNING • LIFE

Kassim Darwish Grammar School for Boys

E Safety Policy

CONTENTS

1.0 PURPOSE OF THE POLICY

This policy defines and describes the acceptable use of IT for staff and students at KD Grammar School for Boys. 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 to minimise the risk to the IT network and systems.

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

This policy must be read in conjunction with the Safeguarding and Child Protection Policy and the Behaviour Policy.

2.0 ROLES AND RESPONSIBILITIES

The Trust Board is responsible for ensuring that its employees, act in a lawful manner, making appropriate use of school technologies for approved purposes only.

The Trust Board is responsible for implementing relevant policies and the school Executive Head Teacher is responsible for ensuring that staff are aware of their contents.

The school Executive Headteacher is responsible for maintaining an inventory of IT equipment as part of the school asset management register and recording to whom it has been issued.

If the school Executive Head Teacher has reason to believe that any IT equipment has been misused by an adult, s/he will consult the Trust for advice without delay. The Trust will agree with the school Executive Head Teacher an appropriate strategy for the investigation of the allegations and liaison with other agencies as appropriate. Incidents will be investigated in a timely manner in accordance with agreed procedures. The Executive Head Teacher will make it clear that internal school staff should not carry out any investigations unless they are both qualified and authorised to do so.

The trustees will ensure that all staff have training on on-line safety.

It is also important to recognise that e-safety is not an IT issue. It may involve the use of IT, but it is about protecting children and young people from harm. If you have a concern about actual, significant harm to a child or young person, or the risk of significant harm, then you should make immediate contact with the Designated Safeguarding Lead (DSL) in the school.

3.0 IT USER RESPONSIBILITIES

Use of KD Grammar School IT resources is granted based on acceptance of the following specific responsibilities:

I. Use only those computing and information technology resources for which you have authorisation.

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 and password 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

II. 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 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 commercial purposes
- to use electronic resources for personal use at inappropriate times or in inappropriate locations
- to attempt to circumvent security mechanisms

III. Protect the access and integrity of computing and information technology resources.

For example: it is a violation

- To intentionally release any malware that damages or harms a 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 deliberately degrade performance or deny service
- to corrupt or misuse information
- to alter or destroy information without authorisation

IV. Abide by applicable laws and school policies and respect the copyrights and intellectual 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

V. 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, without permission
- to access or attempt to access another individual's password or data without explicit authorisation from a senior member of staff, with the direct knowledge of the school Executive Head Teacher.

All staff will be required to sign an agreement each September (or on starting if during a school year) to indicate that they have read and understood these responsibilities. (See Appendix 2) The signed copy will be kept with the IT Manager.

4.0 REPORTING

Staff are responsible for reporting every breach of e-safety. If a member of staff 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 in the Executive Head Teacher

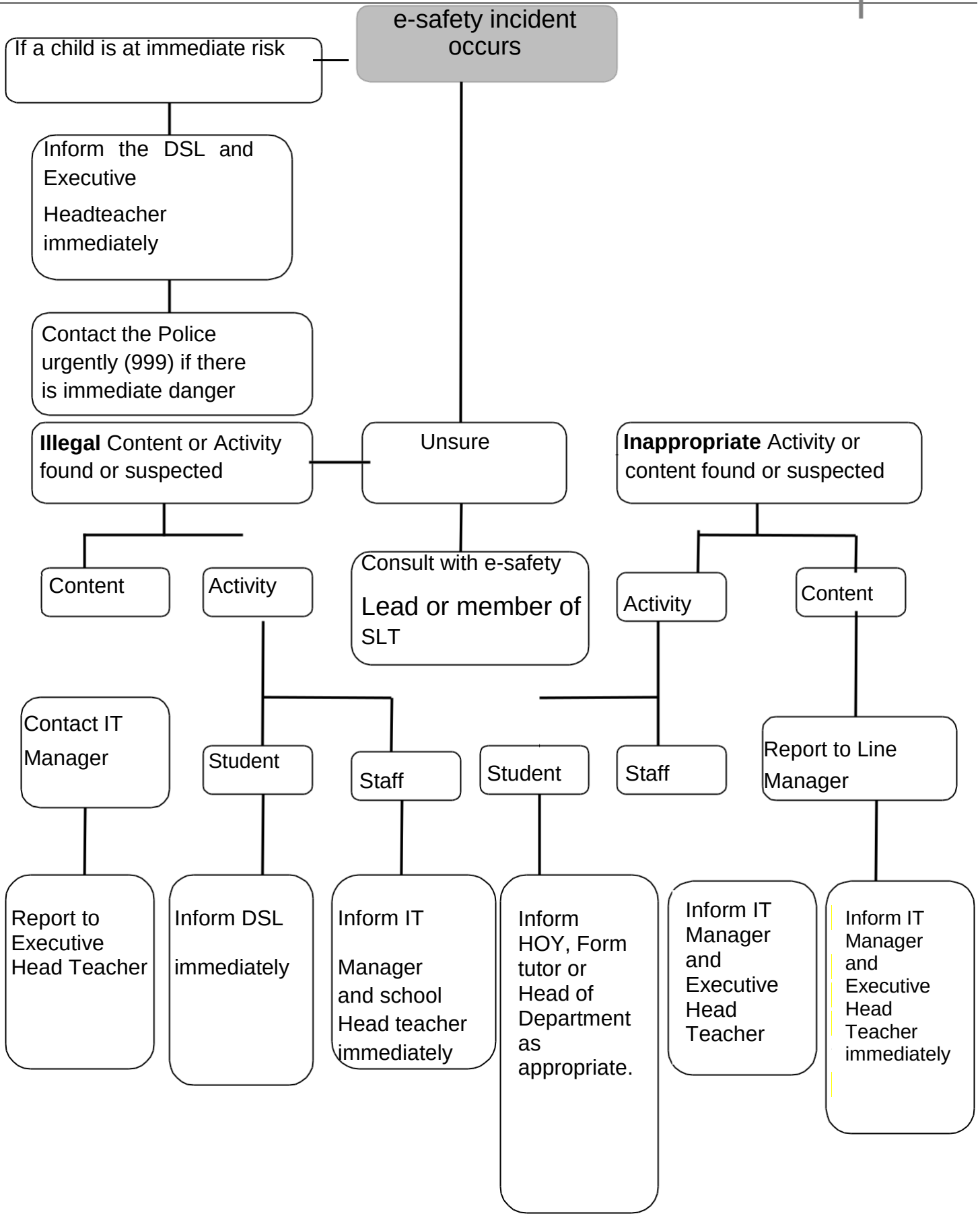
Immediate reporting:

Safeguarding incident	to DSL
Inappropriate activity by a member of staff	to IT Manager
Illegal content or material which requires immediate removal or blocking	to IT Manager

Same day reporting:

Inappropriate material which requires additional filtering on the Internet	to IT Manager
Inappropriate activity by a student in a lesson (which does not constitute a safeguarding incident)	to Head of Department
Inappropriate activity by a student not in a lesson (which does not constitute a safeguarding incident)	to Head of Year

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 behaviour systems.


e-safety incident occurs
If a child is at immediate risk
Inform the DSL and Executive Headteacher immediately
Contact the Police urgently (999) if there is immediate danger
Unsure
Illegal Content or Activity found or suspected
Inappropriate Activity or content found or suspected
Consult with e-safety Lead or member of SLT
Content
Activity
Activity
Content
Contact IT Manager
Student
Staff
Student
Staff
Report to Line Manager
Report to Executive Head Teacher
Inform DSL immediately
Inform IT Manager and school Head teacher immediately
Inform HOY, Form tutor or Head of Department as appropriate.
Inform IT Manager and Executive Head Teacher
Inform IT Manager and Executive Head Teacher immediately

5.0 ACCEPTABLE AND UNACCEPTABLE USE

The rapid developments in hardware and software mean that use of technology changes at an unprecedented rate. It would be impossible to document every potential use of IT equipment in school.

Within the school, we believe that the use of 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, which open up new opportunities for everyone. These technologies can be used to encourage discussion, provide outlets for creativity and enrich the curriculum.

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 come across unsavory, distressing or offensive materials on the Internet and some social networking sites offer cover for unscrupulous individuals to groom children. It is crucial that whilst 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 which is; 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.

Acceptable use is therefore taken to mean the use of the resources to; create imaginative learning opportunities, efficient business practice, continuing professional development and other uses which enable staff to maintain a healthy work-life balance.

6.0 EQUIPMENT AND SERVICES SUMMARY

IT Equipment – the term relates to any equipment provided by school including computers, portable devices and phones.

Any equipment must be used with care and take precautions to ensure it is left ready for other users when finished. Damaged, broken or missing equipment must be reported immediately to the relevant person.

Network logon and password – All users are issued with a user name and password with access rights tailored for their use of the IT systems in school provided they accept the responsibilities outlined in Appendix 2. (IT user responsibilities)

All users must access the network only using their own logon and password. Passwords must not be disclosed or shared. The user assumes full responsibility for the use or misuse of this account.

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; 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 in accordance with the reporting procedures.

Email – An email account is provided to each member of staff and student.
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 and network activity 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 achievements.
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 which are 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 – There is a large amount of personal and sensitive data held on the school systems regarding students, staff and trustees. All adults will ensure that they 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 Own Device (BYOD) – Staff are permitted to use their own personal IT equipment in school at the discretion of the school Executive Head Teacher. 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 or the Trust.

It is the responsibility of the member of staff to ensure that any device brought into school by them is used appropriately and within the scope of this policy. The member of staff is responsible for any use or misuse of this device whilst it is on school grounds or if it is being used for a work-related activity. You are responsible for ensuring that any use adheres to the Data Protection procedures outlined in Section 7 (Safer Social Networking).

7.0 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.

a) 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.
b) In their own interests, adults within school settings need to 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.
c) 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.
d) As security settings change frequently, all staff are encouraged to regularly check that accounts remain secure.
e) 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 may continue to attend the school.
f) Friend/contact requests from any student on roll at the time must be declined and reported to the HOY.
g) Staff should never use or access social networking pages of students unless specifically directed to do so by the head Teacher as part of an investigation
h) 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, the Trust, their colleagues, students or members of the public.
i) 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, the Trust could result in disciplinary action being taken against them.
j) Adults within the school setting must never post derogatory remarks or offensive comments on-line or engage in on-line activities which may bring the school into disrepute or that could be interpreted as reflecting negatively on their professionalism.

Student use of online chat rooms, social networking sites, instant messaging services and text messaging will not be allowed until the school community agrees that these technologies can be supervised or monitored in a way that will guarantee the e-safety of the students.

8.0 COMMUNICATIONS AND SOCIAL CONTACT

a) Adults should keep their personal phone numbers, work login or passwords and personal 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.
b) Adults must understand who is allowed to view the content on their pages of any sites they use and how to restrict access to certain groups of people.
c) Communication between students and adults by whatever method, must take place within clear and explicit professional boundaries. Staff should use their school email for all contact with students.
d) Adults must not request, or respond to, any personal information from a student.
e) 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.
f) 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 only be used in accordance with the school's policy.
g) 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 within the school setting.
h) 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.
i) Any concerns must be raised with the Executive Head Teacher at the earliest opportunity.

9.0 ACCESS TO INAPPROPRIATE IMAGES

a) 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 a significant and potential threat to children. This will lead to criminal investigation and disciplinary action. Where indecent images of children are found, the Executive Head Teacher must be informed immediately.
b) 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 raise serious concerns about the suitability of the adult to continue to work with children.
c) 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 IT Manager immediately.
d) 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 DSL before any investigation is conducted.

10.0 CYBERBULLYING

Cyber bullying is bullying through the use of communication technology like mobile phone text messages, e-mails or websites. This can take many forms for example:

- Sending threatening or abusive text messages or e-mails, personally or anonymously

- Making insulting comments about someone on a website, social networking site (eg MySpace) or online diary (blog)
- Making or sharing derogatory or embarrassing videos of someone via mobile phone or e-mail (such as 'Happy Slapping' videos)

There are many types of cyber-bullying. Although there may be some of which we are unaware, here are some of the more common:

- Text messages – that are threatening or cause discomfort – also included here is "Bluejacking" (the sending of anonymous text messages over short distances using "Bluetooth" wireless technology.
- Picture/video-clips - via mobile phone cameras – images sent to others to make the victim feel threatened or embarrassed.
- Mobile phone calls – silent calls or abusive messages; or stealing the victim's phone and using it to harass others, to make them believe the victim is responsible.
- Emails – threatening or bullying emails, often sent using a pseudonym or somebody else's name.
- Chat room bullying – menacing or upsetting responses to persons (children, young people or adults), when they are in web-based chat room.
- Instant messaging (IM) – unpleasant messages sent while children conduct real- time conversations online using MSM (Microsoft Messenger) or Yahoo Chat; although there are others.
- Bullying via websites – use of defamatory blogs (web logs), personal websites and online personal "own web space" sites such as Bebo (which works by signing on in one's school, therefore making it easy to find a victim) and Myspace – although there are others.

It should be noted that the use of ICT to bully could be against the law. Abusive language or images, used to bully, harass or threaten another, whether spoken or written (through electronic means) may be libellous, may contravene the Harassment Act 1997 or the Telecommunications Act 1984 for example. It should be noted that the use of the web, text messages, e-mail, video or audio to bully another pupil or member of staff will not be tolerated. Full details can be found on the Anti bullying Policy.

11.0 DATA PROTECTION

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 Executive Head Teacher and teachers at the school, other employees at the school or the Trust, or those contracted by the Trust, 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 Executive Head Teacher before actioning.

- Users must access the network only using their own logons 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 of Bromcom 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 Bromcom 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 Executive Head Teacher.
- If a member of staff suspects that a colleague is in breach of the Data Protection Act, he/she must seek clarification from their Line Manager and/or report it to the Executive Head Teacher.
- 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 may not be transferred outside the UK unless as part of a managed, organised move, co-ordinated by the Inform IT Manager and Executive Head Teacher .
- Personal data may not be sent to any third party unless they are a designated organisation, covered by the School's entry in the GDPR/privacy policy.
- The Trust 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 IT manager or the Executive Head Teacher.

APPENDIX 1

12.0 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 Bromcom 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 Executive Head Teacher.
- 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 iPads. 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

- 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)
- When using their personal mobile phone staff are expected to use the school WIFI to access the Internet during school time and on school property. 3G/4G/5G is not permitted as this by-passes the security systems set in place to protect individuals.
- Students are prohibited from the use of their mobile phones on school premises
- 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 e-mail 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 IT Manager and a note of the offending website address (URL) taken so that it can be blocked.
- Internet and e-mail 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 e-mail 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 IT Manager 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 e-mails 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 e-mails sent from an establishment/service e-mail 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 e-mails are received, this must be reported immediately to a trusted adult or member of staff within the service / establishment. E-mails received should 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 unblocked for staff but should only be accessed at appropriate times.
- 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 networking site.
- 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' (Section 7).

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 Bromcom.
- 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.
- 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 on-line gaming forums and must refuse invitations from current students.

APPENDIX 2

13.0 IT USER RESPONSIBILITIES

(Staff initials each line please)

I agree to only use only those computing and information technology resources for which I have authorisation

_____

I agree to only use computing and information technology resources only for their intended purpose.

_____

I agree to protect the access and integrity of computing and information technology resources.

_____

I will abide by applicable laws and school policies and respect the copyrights and intellectual property rights of others, including the legal use of copyrighted software.

_____

I will respect the privacy and personal rights of others.

_____

By accepting the IT user responsibilities, you agree:

1. You have read and agree to follow the procedures laid out in the school's e-safety policy
2. That you understand that e-safety is an important aspect of child protection and you will report any concerns to the relevant staff as per the guidelines
3. That the term 'ICT equipment' applies to any computer, phone or mobile electronic equipment belonging to you or the school
4. You may be subject to disciplinary procedures if found to be in breach of the procedures laid out
5. You will take reasonable steps to ensure that, when using the ICT facilities, all personal data, the school network and the school computer systems are protected from deliberate or accidental damage or disclosure, whether using the system in school or through a remote login
6. To report any breaches of e-safety to the relevant person
7. That you understand that you may be subject to legal proceedings if you are in breach of the Data Protection Act or any other legislation in place to protect the individual
8. That you understand that your files and e-mails may be accessed by the Executive Head Teacher (or designated person) without my prior consent
9. That you will not attempt to by-pass security systems or make illegal copies of files or software
10. That if you use social media sites, you will maintain a professional presence at all times

Staff Signature Date

APPENDIX 3

14.0 DEVICE RESPONSIBILITY CONTRACT AND CONSENT (Signed on receipt of school device)

Staff Name

I acknowledge receiving a for use while I remain in the employment of MIET Ltd. I have read the school e-safety policy. In order to maintain this privilege, I agree to the following responsibilities:

(Staff initial each line please)

_____ I agree to keep this device in my possession at all times. I will not give or lend it to anyone except to return it to the school for upgrades, network connection or repair in case it is damaged.

_____ I agree not to leave this device on view in my car when it is left unattended.

_____ I agree to carry this device in a padded case or backpack, to minimise the chances that it will be damaged or destroyed.

_____ I agree to read and follow the school's e-safety Policy, and will not use this device, in or out of school, for unacceptable or unlawful purposes.

_____ I agree to turn in my device to the school whenever requested for occasional maintenance, updates, or repairs.

_____ I understand that if my device is lost or stolen, I will immediately notify the School.

_____ I agree to return this device to the school before I leave the school

I understand that failure to comply with any of these rules and policies will result in the suspension of my use of this laptop. Restoration of this privilege will require the involvement of the Executive Head Teacher.

Staff Signature Date

Checked by IT Manager

APPENDIX 4

Internet Use Agreement for Student

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. For my own personal safety:

- I understand that KD Grammar will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger" (i.e. where unknown people attempt to make contact and establish interaction), when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.).
- I will not arrange to meet people off-line.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the School's systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use.
- I will not make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the School's systems or devices for on-line gaming, on-line gambling, internet shopping, or video broadcasting (e.g. YouTube), unless I have permission from a member of staff.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the School has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will not use my own personal devices (mobile phones/USB devices etc.) in without specific permission.
- I understand the risks and will not upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes). I will inform a member of staff about my concerns.
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will not use social media sites at any given time within school.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download copies (including music and videos)

- When I am using the internet to find information, I will take care to check that the information that I access is accurate and truthful.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the School has the right to take action against me if I am involved in inappropriate behaviour (that are covered in this agreement) when I am out of school and where they involve my membership of the School (e.g. cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Internet Use Agreement, I may be subject to disciplinary action. This may include loss of access to the school network/internet, detentions, suspensions and contact with parents and in the event of illegal activities involvement of the police.
- I understand I may have my phone or other internet/web enabled devices inspected when requested by school.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Internet Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems.

Parent/Carer Declaration

I have read the Internet Use Agreement with my son.

I give permission for access to the Internet on the terms set out for the duration that my child attends KD Grammar School for Boys.

I consent to the monitoring and auditing of my child's mail and Internet Access.

I have shared this information with my child and will remind them of responsible Internet use throughout their time at school.

Name of student _____Form: _____
Signed Parent/Carer _____
Date _____

Date	September 2023
Reveiwed by	Dr Ghidaoui
Next Review Date of this Policy	September 2024