EDGBASTON
HIGH SCHOOL *for* GIRLS

E-safety: Complete Policy

EDGBASTON
HIGH SCHOOL *for* GIRLS

E-Safety Policy

INTRODUCTION

Reference to the Data Protection and Privacy Policy, Pupils use of Social Media Policy, Social Media Guidelines and Whole School ICT policy and IPAD Acceptable Use Policy would also be appropriate when reading this document.

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

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- E-mail, Instant Messaging and chat rooms
- Social Media, including Facebook and Twitter
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality including ipads.
- Gaming, especially online
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements

At Edgbaston High School, we understand the responsibility to educate our pupils on eSafety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for the school to use technology to benefit learners.

Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, council members, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

EDGBASTON
HIGH SCHOOL *for* GIRLS

eSafety: General

As eSafety is an important aspect of strategic leadership within the school, the Head Teacher and Council have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named eSafety co-ordinator in this school is Anne Lacey who has been designated this role as a member of the School Management Team. All members of the school community have been made aware of who holds this post. It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance

Senior Management and Council are updated by the Head/ eSafety co-ordinator and all Council members have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PSHE.

Edgbaston High school will follow the guidelines provided by the **Office of the Children's eSafety Commissioner (see appendix 1)** when disseminating information to pupils and parents about the age appropriate use of social media platforms and will at all times discourage pupils from using these platforms during the school day

<u>eSafety in the Curriculum</u>

ICT and online resources are increasingly used across the curriculum. We believe it is essential for eSafety guidance to be given to the pupils on a regular and meaningful basis. eSafety is embedded within our curriculum and we continually look for new opportunities to promote eSafety.

- The school has a framework for teaching internet skills in ICT.
    - In Years 1 & 2 when using the internet (specifically images), the staff ask pupils to inform them of anything they see as offensive or do not like. They are also encouraged to do the same when at home with parents. Normally pupils are given the website address to use when doing some research or activity which has been checked by staff.
    - In Years 3 & 4 they look at and discuss eSafety. They have a 'Rules for using the EHS Computer Network' document in their school Diary covering personal details in various scenarios and when using various devices. This is explained and discussed within an appropriate lesson.
    - In Year 5 pupils look at cyberbullying. They also discuss the advantages and disadvantages of technology (phones, computers, cameras etc.) and how they may be used in relation to Cyberbullying. The pupils then look at a quiz on this topic and various

scenarios are also looked at in relation to cyberbullying and discussions of how this could be avoided and dealt with are considered.

- In Year 6 within the autumn term in PSHEE they look at the dangers in relation to eSafety. They primarily look at the Issues and themes that help in 'Keeping Myself e-safe'. This follows the 'Learning Curve education' support pack.

- In general the Prep also have A4 posters around the school stating the basic 'Rules for Online Safety' as also discussed in the Year 3 & 4 lessons.

- In Year 7 the pupils study "Protecting you and your device", "personal information", "chat rooms" and "cyberbullying".

- In Year 8 pupils learn about "information, validity and bias". They learn about how to check the validity of data on a website, what is meant by bias and how important it is to obtain a variety of sources in order to come to an informed conclusion and how to access and search more accurately and concisely for information using the internet.

- In Year 9 PSHEE they revisit cyberbullying and look at the medias portrayal of body image and stereotyping. They also look at internet safety.

- Educating pupils about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the eSafety curriculum as described above.
- A variety of digital awareness activities and assemblies run throughout the year. They include
    - Digital awareness day year 6 & 7 (every other year)
    - Digital Footprint assembly
    - Safer Internet Day project and assembly
    - Fake news activity KS3
- Digital digest on Friday headlines provides information for both parents and pupils about being digitally aware
- 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, respecting other people's information, safe use of images and other important areas through discussion, and appropriate activities
- Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. 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 Cybermentors, Childline
- Pupils are taught to critically evaluate materials and learn good searching skills through discussions and via the ICT curriculum as described above.

<u>eSafety Skills Development for Staff</u>

- Our staff receive regular information and training on eSafety and how they can promote the 'Stay Safe' online messages in the form of in house training at staff meetings and training days.
- Details of the ongoing staff training programme can be found with SEE
- New staff receive information on the school's acceptable use policy as part of their induction
- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the school community
- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas

Managing the School eSafety Messages

- We endeavour to embed eSafety messages across the curriculum whenever the internet and/or related technologies are used
- Assembly
- Friday Headlines
- The eSafety policy will be introduced to the pupils at the start of each school year
- eSafety posters are prominently displayed
- The key eSafety advice will be promoted widely throughout the school.

Incident Reporting, eSafety Incident Log & Infringements

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the Head Teacher or eSafety Co-ordinator. Additionally, all security breaches, lost/stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the Head Teacher.
Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety co-ordinator
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the eSafety co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart)
- Users are made aware of sanctions relating to the misuse or misconduct by reference to the policies on misconduct which are available to all staff.

EDGBASTON
HIGH SCHOOL *for* GIRLS

eSafety: Computer Viruses

All files downloaded from the Internet, received via e-mail or on removable media such as a memory stick must be checked for any viruses using school provided anti-virus software before being used

- Never interfere with any anti-virus software installed on school ICT equipment that you use
- If your machine is not routinely connected to the school network, you must make provision for regular virus updates through the Network Manager.
- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact the Network Manager immediately.
- The Network Manager sends regular emails about potential threats to all users. It is the user's responsibility to check these.

EDGBASTON
HIGH SCHOOL *for* GIRLS

eSafety: Disposal of ICT Equipment

All redundant ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data. As far as possible Edgbaston High School will endeavour to recycle as much of it's hardware as possible.

- All redundant ICT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this will happen
- Disposal of any ICT equipment will conform to:
  The Waste Electrical and Electronic Equipment Regulations 2006
  The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007
  Data Protection Act 1998
  Electricity at Work Regulations 1989
- The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal
- The school's disposal record will include:
  Date item disposed of
  Authorisation for disposal, including:
  Verification of software licensing
  Any personal data likely to be held on the storage media? *
  How it was disposed of eg waste, gift, sale
  Name of person & / or organisation who received the disposed item

  * if personal data is likely to be held the storage media will be over written multiple times to ensure the data is irretrievably destroyed.
- Any redundant ICT equipment being considered for sale / gift will have been subject to a recent electrical safety check and hold a valid PAT certificate

EDGBASTON
HIGH SCHOOL *for* GIRLS

eSafety: e-Mail

The use of e-mail within Edgbaston High School is an essential means of communication for both staff and pupils. In the context of school, e-mail should not be considered private.

Managing e-Mail

- The school gives all staff their own e-mail account to use for all school business as a work based tool. This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses
- The school requires a standard disclaimer to be attached to all e-mail correspondence, stating that, 'the views expressed are not necessarily those of the school'. The responsibility for adding this disclaimer lies with the member of staff. If you have any concerns about how to carry out this action then please see the ICT staff or the Network Manager for advice.
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper. Anything of a sensitive nature should be checked by the Head in the same way as a letter.
- Staff sending e-mails to external organisations, parents or pupils are advised to cc. the Headteacher or their line manager.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes
- E-mails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your e-mail account as follows:
    - Delete all e-mails of short-term value
    - Organise e-mail into folders and carry out frequent house-keeping on all folders and archives
- All pupils in the Senior School have their own individual school issued accounts
- The forwarding of chain letters is not permitted in school
- All pupil e-mail users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments
- Pupils must immediately tell a teacher if they receive an offensive e-mail
- Staff must inform the eSafety co-ordinator or their line manager if they receive an offensive e-mail
- Pupils are introduced to e-mail as part of the ICT Scheme of Work
- However the school e-mail is accessed (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply

Sending e-Mails

- Use your own school e-mail account so that you are clearly identified as the originator of a message
- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate
- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments
- School e-mail is not to be used for personal advertising

Receiving e-Mails

- Check your e-mail regularly
- emails can have the 'out-of-office' notification attached when away for extended periods by Senior Staff.
- Never open attachments from an untrusted source; Consult the Network Manager first
- Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder
- The automatic forwarding and deletion of e-mails is not allowed by individuals.

e-mailing Personal, Sensitive, Confidential or Classified Information

- In the case of sensitive data it is strongly advised that you:
  - Obtain express consent from your line manager to provide the information by e-mail
  - Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:
  - Verify the details, including accurate e-mail address, of any intended recipient of the information
  - Verify (by phoning) the details of a requestor before responding to e-mail requests for information
  - Do not copy or forward the e-mail to any more recipients than is absolutely necessary
  - Do not send the information to anybody/person whose details you have been unable to separately verify (usually by phone)
  - Do not identify such information in the subject line of any e-mail
  - Request confirmation of safe receipt

E-mails with attachments

- Staff and Pupils are advised as much as possible to avoid emailing documents but to use sharepoint in order to disseminate and share information.
- Reducing the numbers of copies of a document in circulation minimises the risk of a data breach, reduces the number of emails circulating and alleviates the stress of managing document storage

EDGBASTON
HIGH SCHOOL *for* GIRLS

eSafety: Safe use of Images

This policy is to be read in conjunction with the 'Taking and Storing Images of Pupils Policy' and Data Protection and Privacy Policy

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

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment. There is an opt out process for parents.
- Staff are not recommended to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device.
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of pupils, staff and others without advance permission from the Headteacher.
- Pupils and staff must have permission from the Headteacher before any image can be uploaded for publication Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes. This is very important with the introduction of ipads into the school environment.
- Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students / pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

On a child's entry to the school, all parents/carers 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, ie exhibition promoting the school

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 or carers may withdraw permission, in writing, at any time.

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.

Only the Web Manager (Annelle Rowlands) has authority to upload to the site.

Storage of Images

- Images/ films of children are stored on the school's network
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Headteacher
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network or other online school resource
- The Network Manager and the Heads of Department have the responsibility of archiving the images when they are no longer required, or when the pupil has left the school. The images should be reviewed at least once a year.

Webcams and CCTV

- The school uses CCTV for security and safety. The only people with access to this are RW, SH, SW, LB, and GF)
- We do not use publicly accessible webcams in school

EDGBASTON
HIGH SCHOOL *for* GIRLS

eSafety: Internet Access

The internet is an open worldwide communication medium, available to everyone, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

Managing the Internet

- The school provides pupils with supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet connectivity
- Staff will preview any recommended sites before use where possible.
- Raw image searches are discouraged when working with pupils
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. Parents will be advised to supervise any further research
- Where students / pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- All users must observe software copyright at all times
- All users must observe copyright of materials from electronic resources

Internet Use

- Do not reveal names of colleagues, pupils, others or any other confidential information acquired through your job on any social networking site or other online application
- On-line gambling or gaming is not allowed
- It is at the Headteacher's discretion as to what internet activities are permissible for staff and pupils and how this is disseminated.
- Our school also employs some additional web-filtering which is the responsibility of the Network Manager.
- Edgbaston High School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required
- The school does not allow pupils access to internet logs
- The school uses management control tools for controlling and monitoring workstations
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety coordinator or teacher as appropriate
- It is the responsibility of the school, by delegation to the Network Manager, to ensure that anti-virus protection is installed and kept up-to-date on all school machines

- Pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility nor the Network Manager's to install or maintain virus protection on personal systems. If pupils wish to bring in work on removable media it must be given to the ICT technicians for a safety check first
- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the Network Manager.
- If there are any issues related to viruses or anti-virus software, the Network Manager should be informed by contact by telephone on extension 238.

EDGBASTON
HIGH SCHOOL *for* GIRLS

eSafety: Monitoring

Authorised ICT staff may inspect any ICT equipment owned or leased by the school at any time without prior notice

ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of school ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

ICT authorised staff may, without prior notice, access the e-mail or voice-mail account where applicable, of someone who is absent in order to deal with any school or business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

All internet activity is logged and may be monitored by the Network Manager or other staff.

A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual.

Any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure.
Policy breaches may also lead to criminal or civil proceedings.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the Head Teacher, Facilities Manager or eSafety Co-ordinator. Additionally, all security breaches, lost/stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the Head Teacher.

The school uses ESAFE to monitor the activity on the network.

The school carries out random inspection of ipads across year groups on a termly basis and when necessary.

EDGBASTON HIGH SCHOOL *for* GIRLS

eSafety: School ICT Equipment

All members of the school are responsible for their activity as a user of ICT equipment.

- The Network Manager logs ICT equipment issued to staff and records serial numbers as part of the school's inventory
- We do not allow users to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT facilities if available
- Staff should ensure that all ICT equipment they use is kept physically secure
- Staff should not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990
- Data should be saved frequently to the school's network.
- Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick or other portable device. If it is necessary to do so the local drive must be encrypted
- A time locking screensaver is applied to all PCs.
- Privately owned ICT equipment should not be used on a school network
- When a member of staff leaves the employment of the school all ICT equipment should be returned to the line Manager.
- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA)
- No-one should charge their mobile phone or ipad in school. If this is really necessary the device should be taken to ICT.

<u>Portable & Mobile ICT Equipment</u>

This section covers such items as laptops, mobile devices and removable data storage devices.

- All activities carried out on school systems and hardware will be monitored in accordance with the general policy
- Staff must ensure that all school data is stored on the school network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted
- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey
- Staff should ensure that portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades
- The installation of any applications or software packages must be authorised by the ICT support team, fully licensed and only carried out by your ICT support
- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight
- Portable equipment must be transported in its protective case if supplied

Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device. The exception to this rule is an occasion such as a PE match where the parent may be contacted by a private phone. This is strongly discouraged.
- Pupils are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes within lesson time. In KS3 and KS4 pupils should switch their mobile phones off and lock them in their locker. If they need to use a telephone they should go to the Reception area. In KS5 girls may have a mobile phone but it should be on silent and not used in lessons.
- The school is not responsible for the loss, damage or theft of any personal mobile device
- The sending of inappropriate text messages between any member of the school community is not allowed
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device

School Provided Mobile Devices (including ipads and phones)

- The sending of inappropriate messages and images between any member of the school community is not allowed. If this occurs the school's behavioural and/or disciplinary procedure will be followed.
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community
- Where the school provides mobile technologies such as phones, laptops and iPads for offsite visits and trips, only these devices should be used
- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school.
- ipads may be used in lessons for research but only those websites to which pupils have been directed by staff may be used.
- ipads have apps pre downloaded by the ICT support staff. Downloading of other apps is discouraged. ipads are currently shared and work should be stored on One Drive for future use and deleted from the ipad at the end of the lesson.

EDGBASTON HIGH SCHOOL for GIRLS

eSafety: Security of Data including Passwords

The school gives relevant staff access to its Management Information System (PASS), with a unique username and password

- It is the responsibility of everyone to keep passwords secure
- Staff are aware of their responsibility when accessing school data
- Staff should keep all school related data secure. This includes all personal, sensitive, confidential or classified data
- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight
- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under supervision at all times

Passwords

- Always use your own personal passwords
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures
- Staff should change temporary passwords at first logon
- Staff should change passwords whenever there is any indication of possible system or password compromise
- Do not record passwords or encryption keys on paper or in an unprotected file
- Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished
- Never tell a child or colleague your password
- If you aware of a breach of security with your password or account inform the Headteacher and the Network Manager immediately
- Passwords must contain a minimum of eight characters and be difficult to guess
- Passwords should contain a mixture of upper and lowercase letters, numbers and symbols
- User ID and passwords for staff and pupils who have left the school are removed from the system within 6 months. This is to allow access to emails and the network which have been used by this individual. Pupils in Year 14 can keep their account open until the beginning of the following calendar year.

Password Security

- Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords private and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.
- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-Safety Policy and Data Security
- Users are provided with an individual network, email, and Management Information System (PASS) log-in username.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others

- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school networks and MIS systems, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked. The normal automatic lock time for the staff account on a PC is 5 minutes.
- Change of passwords is forced every 4 months.

EDGBASTON HIGH SCHOOL *for* GIRLS

eSafety: Servers

Servers should be kept in a locked and secure environment

- The server should be password protected and locked.
- Existing servers should have security software installed appropriate to the machine's specification
- Back up tapes should be encrypted by appropriate software
- Data must be backed up regularly
- Back up tapes/discs must be securely stored in a fireproof container

EDGBASTON
HIGH SCHOOL *for* GIRLS

eSafety: Other Web Technologies including Good Practice by Pupils and Cyberbullying

Online technologies, including social networking may have issues regarding the appropriateness of some content, contact, culture and commercialism.

- At present, the school does not allow access to social networking sites to pupils within the school except for the Sixth Form.
- All pupils are advised to be cautious about the information given by others on such websites, for example users not being who they say they are
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online
- Pupils are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests)
- Our pupils are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts and information online
- Pupils are asked to report any incidents of Cyberbullying to their Head of Year or to the eSafety Officer. The Bullying Policy can be referenced here.
- Staff may only create blogs, wikis or other online areas such as Twitter in order to communicate with pupils using systems approved by the Headteacher and following the 'Social Media Policy'.

<u>Parental Involvement</u>

- We believe that it is essential for parents/carers to be fully involved with promoting eSafety both in and outside of school and to be aware of their responsibilities. We offer discussion sessions and training for parents regarding eSafety.
- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the school. The pupil should sign as well.
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used for example on the school website. This is an opt out process.

EDGBASTON
HIGH SCHOOL *for* GIRLS

School Network Policy: Pupils

General Warning

- Every user must take responsibility for her use of the computer network and Internet and stay away from inappropriate sites. If you mistakenly access inappropriate information on the INTERNET, you should immediately tell your teacher. You must not show or discuss this with others.
- ICT staff will monitor use of the network, Internet and email. Any misuse will result in withdrawal of the privilege of using these.
- Every care is being taken to filter inappropriate sites using Internet filtering software.
- Filtering of the internet while using ipads at home is the responsibility of parents.

Access

- Access to the school network and Internet is available from any network station during the normal school day, and from home via internet.
- All users are required to log-on with their own personal Username. Passwords must not be disclosed to others nor may you use the password belonging to anyone else. You must not use a computer logged-on by another user.
- All users must make sure that they log-off correctly at the end of any session on a computer.
- The use of memory sticks is encouraged but pupils must take responsibility for ensuring that the appropriate virus checks are in place.
- Mobile equipment such as lap tops can be connected wirelessly. It is the individual's responsibility to ensure that adequate virus checks are in place.

Security and Privacy

- Anti-virus software is installed on every server and station and is updated regularly to prevent infection by the Internet, memory sticks and email. Memory sticks are automatically scanned. If a threat is identified you should let your teacher know.

Email

- You may only use the school Outlook email system for school business and may not use any other web based email services such as Hotmail.
- You should not respond to any message that seems inappropriate or makes you feel uncomfortable and you should immediately tell a member of staff if you receive any such message. It is not your fault if you receive such a message.
- Anonymous letters and chain letters are not allowed.
- The school email address cannot be used for political, commercial or private use.
- When using the network you must always treat others with respect. It is unacceptable to transmit offensive or harassing messages.

Internet

- Accessing and/or playing games on the Internet is not allowed unless it can be shown that these have a significant educational value.
- You should never give out personal information such as your name, school name and location, home address, telephone number or send your photograph or arrange to meet anyone you encounter on the Internet.
- The use of social media sites in school is not allowed.
- Users may not access resources for which they do not have permission.
- Use of the Internet in lessons requires the permission of a member of staff.
- Copyright and intellectual property rights must be respected.
- Text, images, sound and video can be copied and saved for educational purposes. You must acknowledge the source of your information. You must not submit work from the internet as your own.
- Users must not download, or attempt to download, program files via the Internet.

Network Use

- Users may not install, attempt to install or store programs of any type on the stations without prior permission from ICT staff. You may download free educational apps onto the ipad which you have been allocated.
- Do not attempt to bypass security or attempt to alter settings in place on the computers.
- The transfer of program files to or from the network is strictly forbidden.
- No food or drinks may be taken into the ICT Department or near any other computers around school.
- The school ICT systems may not be used for private, commercial or political purposes unless permission has been granted by staff.
- You will avoid unnecessary printing. You cannot print in colour without permission. You should carry out a spell check and a print preview before printing.
- You are expected to behave sensibly in the computer rooms and, should a machine be found to be faulty, to report the problem to a member of the computing staff as soon as possible. You are responsible for leaving your immediate work area tidy when you have finished a computer session.

Failure to follow policy

The user's use of the computer network and Internet is a privilege, not a right. A user who violates this policy shall at a minimum, have her access to the computer network and Internet suspended. Access will be terminated following a serious violation. A user violates this policy by her own action or by failing to report any violations by other users that come to the attention of the user. A user violates this policy if she permits another to use her account or password to access the computer network and Internet, including any user whose access has been denied or terminated. The school may delete any inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place. The school may also take other disciplinary action in such circumstances.

Edgbaston High School Network Policy

Please complete and return to Mrs Y Crawford, School Secretary

I have read the policy with my daughter. I understand that failure to follow these rules will result in restrictions of my use of the internet and other ICT activities at school.

Signed: …… (Girl) Form: ……

Signed: …… (Parent)

Please print girl's name: ……

EDGBASTON
HIGH SCHOOL *for* GIRLS

School Network Policy: Staff

This should be read in conjunction with the school network policy which has been signed by all pupils.

General

Passwords should be changed at least once a term and should not be shared with others. Passwords should consist of both digits and letters. All staff have a responsibility to protect the confidentiality and security of the school network. Staff must log off when they have finished with a computer. If staff need to leave a computer unattended for any reason it should be locked.

Individuals are personally responsible for the use and safekeeping of memory sticks and the data held on them.

Use of the Internet and Email

Staff may use email services such as 'Hotmail' but are expected to use the school email system Outlook/Office 365 for school business and to communicate responsibly.

Staff may use the internet for personal use but this privilege should not be abused. Staff are reminded that there is material on the internet which is not appropriate in the school environment and is not in keeping with the professional standards of adults who work with young people. Examples might include soft-core pornography, hate material and material which others may find offensive such as sexist or racist jokes and cartoons.

Specific breach of policy might include deliberately accessing, printing, showing or transmitting inappropriate material within the school's network. There are sanctions for deliberate access to inappropriate materials by staff according to the level of the offence, (for example immediate suspension, possibly leading to dismissal).

Staff use of the senior school network is monitored by ESAFE. This software monitors everything that appears on individual PC screens, whether via the internet, email or in Word™ or any other offline application. If an unacceptable word or phrase is used the Network Manager is notified by the software.

If staff accidentally access inappropriate materials they should immediately inform the Headteacher.

Staff should note that the school cannot be held responsible for any use of the internet eg credit card details.

Private social networking sites should be used carefully and staff are recommended not to make current pupils social contacts.

Using Digital Images and Video

It is essential that staff are aware of the potential risks in the use of images of pupils.

Staff may use their own digital cameras for school use and may then download images onto the school network for school use. Staff are encouraged to delete images once they are finished with or after a maximum of one year. Images on the school network will be archived annually.
When using images you must not use the first and last name of individuals in a photograph. This reduces the risk of unsolicited attention from people outside school. An easy rule to remember is:

- If the pupil is named avoid using their photograph
- If a photograph is used, avoid naming the pupil
- Consider using groups of children rather than individuals
- Ensure that the image is appropriately named – do not use pupil's names in image file names
- Only use images of pupils in appropriate dress to reduce the risk of inappropriate use

Anti-Virus Protection

Staff must scan files brought into school on removable media such as memory sticks before each use using anti-virus software.

Attachments should be scanned before opening them. Anything from an unknown source should not be opened.

EDGBASTON
HIGH SCHOOL *for* GIRLS

I have read and understood the Staff Network Policy.

Signed: _____

Print Name: _____

Date: _____

EDGBASTON
HIGH SCHOOL *for* GIRLS

iPad Acceptable Use Policy

The iPad is provided for educational use.

The policies, procedures and information within this document applies to all iPads used in school. Teachers and other school staff may also set additional requirements for use within their classroom.

Users Responsibilities

You will be provided with an ipad case which you are expected to use.

- The iPad screen is made of glass and therefore is subject to cracking and breaking if misused: Please do not place heavy objects (books, laptops, etc.) on top of the iPad.
- Only a soft cloth or approved laptop screen cleaning solution is to be used to clean the iPad screen.
- Please do not subject the iPad to extreme heat or cold as this can cause damage
- Please do not store or leave unattended in vehicles. It will not be insured.
- The iPad is subject to routine monitoring by Edgbaston High School. The school retains the right to filter internet content and to manage the use and connection of iPads to the school network. Please be aware that you may be asked for the iPad for inspection at any time.
- Users in breach of the Responsible Use Policy may be subject to but not limited to; disciplinary action, confiscation, removal of content or referral to external agencies in the event of illegal activity.
- Edgbaston High School is not responsible for financial loss or any loss of any personal files that may be deleted from an iPad.

Additional Responsibilities for Pupils

- If an iPad is left at home or is not charged, the user remains responsible for completing all schoolwork as if they had use of their iPad.
- Malfunctions or technical issues are not acceptable excuses for failing to complete school work, unless there is no other means of completion.
- Pupils are expected to provide earphones for use with the iPad.
- Pupils must not use their iPad in School corridors on their journeys to and from school.
- Pupils in breach of the Responsible Use Policy may be subject to but not limited to; disciplinary action, confiscation, removal of content or referral to external agencies in the event of illegal activity.
- In the event of any disciplinary action or breakages, the completion of all class work remains the responsibility of the pupil.
- Ipads should be password protected. Pupils are prohibited from sharing this password with anyone else except their parents or a member of staff when requested.

Under no circumstances may any student use anyone else's password.

Camera Use

- Users must use good judgment when using the camera. The user agrees that the camera will not be used to take inappropriate, illicit or sexually explicit photographs or videos, nor will it be used to embarrass anyone in any way. Any use of camera in toilets or changing rooms, regardless of intent, will be treated as a serious violation.
- Users may not photograph any other person, without that person's consent.
- In lessons, use of the camera and microphone is strictly prohibited unless permission is granted by a teacher.

- Images of other people may only be made with the permission of those in the photograph.

Posting school related images or photographs on any site on the internet is strictly prohibited.

Safeguarding and Maintaining as an Academic Tool

- iPads are required to be charged and be ready to use in school.
- Items deleted from the iPad cannot be recovered.
- Space is limited. Academic content takes precedence over personal files and apps.
- The whereabouts of the iPad should be known at all times.
- It is a user's responsibility to keep their iPad safe and secure.
- iPads belonging to other users are not to be tampered with in any manner.
- If an iPad is found unattended, it should be given to the nearest member of staff.

Lost, Damaged or Stolen iPad

- iPads are not insured by the school when not on the school premises.
- If the iPad is lost, stolen, or damaged, the eSafety Officer/Network Manager/Head Teacher must be notified immediately. If the iPad is stolen it must be reported to the police and a Police Crime number obtained.
- iPads that are believed to be stolen can be tracked through iCloud.
- If an iPad is damaged it will be repaired on one occasion, future repairs are the responsibility of the user.

Prohibited Uses (not exclusive):

- Accessing Inappropriate Materials – All material on the iPad must adhere to the ICT Responsible Use Policy. Users are not allow to send, access, upload, download or distribute offensive, threatening, pornographic, obscene, or sexually explicit materials.
- Illegal Activities – Use of the school's internet/e-mail accounts for financial or commercial gain or for any illegal activity.
- Violating Copyrights – Users must adhere to copyright law when downloading content on their iPad.
- Any user caught trying to gain access to another user's accounts, files or data will be subject to disciplinary action.
- Malicious Use/Vandalism – Any attempt to destroy hardware, software or data will be subject to disciplinary action.
- Inappropriate media may not be used as a screensaver or background photo. Presence of pornographic materials, inappropriate language, alcohol, drug or gang related symbols or pictures will result in disciplinary actions.
- Individual users are responsible for the setting up and use of any home internet connections and no support will be provided for this by the school. It is the responsibility of the Parent/Guardian to monitor and oversee iPad use within the home setting.
- You will be required to set up an Apple id at school in order to download the apps which will be provided. The Apple id is not to be used on any personal device – it is only for the school iPad. The school is in no way responsible for any costs which you may incur by purchasing apps. Upgrade versions of licensed Software/Apps are available from time to time. Students will be expected to download all updates prompted by Apple when advised to do so.
- Users should be aware of and abide by the guidelines set out by the School eSafety policy. You may not change iPad settings (exceptions include personal settings such as font size, brightness etc).

EDGBASTON
HIGH SCHOOL *for* GIRLS

The iPad Acceptable Use Policy Agreement

Please complete the form below and return to Mrs Lacey by Friday 26 June.

Summary of Student Agreement for iPad Use:

I will take good care of my iPad.

I will never lend my iPad to others.

I will know where my iPad is at all times.

I will charge my iPad every night and not at school.

I will provide a pair of ear phones for use in school.

I will keep food and drinks away from my iPad since they may cause damage to the device.

I will not disassemble any part of my iPad or attempt any repairs.

I will protect my iPad by only carrying it whilst it is in a case.

I will only use my iPad in ways that are appropriate.

I understand that my iPad is subject to inspection at any time without notice.

I will only photograph people with their permission.

I will only use the camera or the microphone when my teacher tells me to.

I will never share any images or movies of people in a public space on the Internet, unless I am asked to do so by my Teacher.

I will not use my iPad in School corridors or on journeys to and from school

I agree to abide by the statements of the school iPad acceptable use policy

I have read, understand and agree to abide by the terms of the iPad Acceptable Use Policy.

Pupil's Signature: …….. Form……

Pupil's Name: ……..

Date: ……..

Appendix 1

Office of the Children's eSafety Commissioner

Heading

Is there an age limit for kids on social media?

Most social media services and apps require users to be 13 years old to join.

Why 13? This is usually to comply with the Children's Online Privacy Protection Act of 1998 (COPPA)—a US law preventing the collection and storage of personal information from a child under 13.

What about APPS? App stores set their own age ratings based on the app's content.

Body text

Table: Age Guide to Social Media

Social Media	**Terms of Use – Minimum Age Requirements**	**App Store Rating**	**Google Play Rating**
ASK.fm	13+	12+	12+
Club Penguin	All ages (directed at 6 – 14 year olds)	4+	G - General
EA (Electronic Arts)	18+ (with parental permission up to 17 yrs)	n/a	G - general
Facebook	13+	4+	12+
Facebook Messenger	13+	4+	3+
Flickr	13+	12+	12+
Foursquare	13+	4+	12+
Google+	13+	17+	12+
Instagram	13+	12+	12+
Keek	13+ (with parental permission up to 17 yrs)	12+	12+
Kik	13+ (with parental permission up to 17 yrs)	12+	12+
Linkedin	14+	4+	3+
Minecraft	All ages (parental permission required to create a mojang account if user is under 13 yrs)	n/a	M – Mature (Pocket Edition)
Moshi Monsters	All ages (Directed at 6 – 12 year olds. If user is under 13, parent's email is required)	4+	G - General

Pinterest	13+	12+	12+
Skype	18+ (With parental permission up to 17 yrs)	4+	3+
Snapchat	13+	12+	12+
Spotafriend	13-19 yrs only	17+	16+
Steam	13+	17+	12+
Tinder	18+ (Facebook account required to register)	17+	18+
Tumblr	13+	17+	12+
Twitter	13+	4+	12+
Vimeo	13+ (With parental permission up to 17 yrs)	17+	12+
Vine	13+	17+	12+
WhatsApp	16+	4+	3+
Yellow	13+ (With parental permission up to 17 yrs)	12+	12+
YouTube	13+	17+	12+

* Age guide based on published Terms of Use and app store ratings as at April 2016.

esafety.gov.au/iparent