EDGBASTON HIGH SCHOOL

E-Safety Policy

Rationale

The internet and associated devices, such as computers, tablets, mobile phones, and games consoles, are an important part of everyday life. However, these modern technologies have created a landscape of challenges and dangers that is still constantly changing. To ensure that the school provides a safe environment for learning, we adhere to the following principles:

- Online safety is an essential part of safeguarding, and the school has a duty to ensure that all pupils and staff are protected from potential harm online.
- Online safety education is an important preparation for life. Pupils should be empowered to build resilience and to develop strategies to prevent, manage and respond to risk online.

The issues classified within online safety are considerable, but can be broadly categorised into four areas of risk:

- Content: being exposed to illegal, inappropriate, or harmful material; for example, pornography, racist or radical and extremist views, and in some respects fake news.
- Contact: being subjected to harmful online interaction with other users; for example, children can be contacted by bullies or people who groom or seek to abuse them.
- Commercial exploitation: for example, young people can be unaware of hidden costs and advertising in apps, games, and website.
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending, and receiving explicit images, or online bullying.

This policy applies to all staff including teachers, support staff, external contractors, visitors, volunteers, and other individuals who work for, or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as pupils and parents/carers. It applies to the whole school including the Early Years Foundation Stage. It applies to access to school systems, the internet, and the use of technology, using devices provided by the school or personal devices. The policy also applies to online safety behaviour such as cyber-bullying, which may take place outside the school, but is linked to membership of the school. The school will deal with such behaviour within this policy and associated behaviour and discipline policies, and will, where known, inform parents/carers of incidents of inappropriate online behaviour that take place out of school.

Links to other policies

- Data Breach Management Policy
- Data Protection & Privacy Policy
- Safeguarding and Child Protection Policy
- Staff Behaviour Policy (which incorporates Staff Code of Conduct)
- Acceptable Use Agreements (AUAs) for Pupils, Staff, Volunteers & Governors
- Behaviour Policy
- Anti-Bullying Policy
- Early Years Foundation Stage (EYFS)
- Acceptable Use Policy

Please see the end of this policy for all the acceptable usage agreements.

Objectives

- To enable all staff to work safely and responsibly to model positive behaviour online and to manage professional standards and practice when using technology.
- To identify approaches to educate and raise awareness of online safety throughout the community
- To identify clear procedures to use when responding to online safety concerns.
- To ensure that the whole school has the knowledge to stay safe and risk free whilst online.

Success Criteria

- All members of the school's community safeguarded and protected online.
- Risks are identified, assessed, and mitigated (where possible) and the risk of harm to the student or liability to the school reduced.

Methodology

1. **Implementation**

Education and engagement with pupils

The school curriculum includes age-appropriate lessons and activities on online safety for all pupils, intended to raise awareness, build resilience, and promote safe and responsible internet use by:

- Ensuring education regarding safe and responsible use precedes internet access.
- Including online safety across the curriculum, including the Personal Social and Health Education, Relationships and Sex Education and Computing programmes of study, covering use both at school and home.
- Reinforcing online safety messages whenever technology or the internet is in use.
- Ensuring that the needs of pupils considered to be more vulnerable online, such as those with SEND or mental health needs, are met appropriately.
- Using support, such as peer education approaches and external visitors, to complement online safety education in the curriculum.
- Educating pupils in the effective use of the internet to research; including the skills of knowledge location, retrieval, and evaluation.
- Teaching pupils to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Teaching pupils to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Supporting students in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making

  The school will support pupils to read and understand the Acceptable Use Agreement in a way which suits their age and ability by:
- Discussing the ICT Acceptable Use Agreement implications. Reinforcing the principles via display, classroom discussion etc.
- Informing pupils that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
- Recognising positive use of technology by pupils.

Training and engagement with staff

The school will:

- Provide and discuss the E-Safety Policy and staff Acceptable Use Agreement with all members of staff as part of induction.

- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates.
- Make staff aware that school systems are monitored, and activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with school's policies when accessing school systems and devices.
- Make staff aware that their online conduct out of school, including personal use of social media, could have an impact on their professional role and reputation within school
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the pupils
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting pupils, colleagues, or other members of the school community.

Awareness and engagement with parents and carers

Parents and carers have an essential role to play in enabling children to become safe and responsible users of the internet and associated technologies. The school will build a partnership approach to online safety with parents and carers by:

- Providing information and guidance on online safety in a variety of formats. This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings.
- Drawing parents' attention to the school online safety policy and expectations in newsletters and on the website.
- Requiring parents to read the pupil Acceptable Use Agreement and discuss its implications with their children.

Reducing Online Risks

The internet is a constantly changing environment with new apps, devices, websites, and material emerging at a rapid pace. The school will:

- Regularly review the methods used to identify, assess, and minimise online risks.
- Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in school is permitted.
- Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
- Ensure, through online safety education and the school AUAs, that pupils know that the school's expectations regarding safe and appropriate behaviour online apply whether the school's networks are used or not.

2. Monitoring

Responding to Online Safety Incidents and Concerns

- All members of the school community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), self-generated sexual abuse as a result of online grooming, cyberbullying and illegal content.
- All members of the community must respect confidentiality and the need to follow the official school procedures for reporting concerns.
- Incidents will be managed depending on their nature and severity, according to the relevant school policies.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes in policy or practice as required.
- If the school is unsure how to proceed with an incident or concern, the DSL will seek legal advice.
- Where there is suspicion, that illegal activity has taken place, the school will contact the Police using 101, or 999 if there is immediate danger or risk of harm.

- If an incident or concern needs to be passed beyond the school community (for example if other local schools are involved or the public may be at risk), the school will speak with the Police and/or the Local Authority first, to ensure that potential investigations are not compromised.

Concerns about Pupils' Welfare

- The DSL will be informed immediately of any online safety incident that could be considered a safeguarding or child protection concern.
- The DSL will ensure that online safeguarding concerns are escalated and reported to relevant agencies.
- The school will inform parents and carers of any incidents or concerns involving their child, as and when required.

Misuse

- Complaints about IT misuse by pupils will be dealt with by a senior member of staff under the relevant policies and procedures and according to the nature of the complaint.
- Any complaint about staff misuse will be referred to the Headteacher.
- Pupils and parents are informed of the school's complaints procedure.

Evaluation and Review

The school will monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied in practice.

The policy framework will be reviewed by Edgbaston High School at least annually, and in response to any new national guidance or legislation, significant developments in the use of technology, emerging threats or incidents that have taken place.

Signed by the Headmistress: CAMacro

Approved by
The Governing Body

Approved by the Governing Body:

Date: 13/1/25

Review Date: January 2026

Appendix 1: Roles and Responsibilities

- Antonietta Cirillo-Campell is the Designated Safeguarding Lead (DSL) responsible for online safety
- All members of the community have important roles and responsibilities to play regarding online safety.

The Headteacher:

- Has overall responsibility for online safety provision.
- Ensures that online safety is viewed as a safeguarding issue and that practice is in line with Edgbaston High School's and national recommendations and requirements.
- Ensures the school follows the school's policies and practices regarding online safety (including the Acceptable Use Agreements), information security and data protection.
- Ensures that online safety is embedded within the whole school curriculum, which enables all pupils to develop an age-appropriate understanding of online safety.
- Supports the DSL by ensuring they have sufficient training, time, support, and resources to fulfil their responsibilities.
- Ensures that all staff receive regular, up to date and appropriate online safety training.
- Is aware of what to do in the event of a serious online safety incident and will ensure that there are robust reporting channels for online safety concerns, including internal and national support.
- Receives regular reports from the DSL on online safety.
- Ensures that online safety practice is audited and evaluated regularly to identify strengths and areas for improvement.

The Designated Safeguarding Lead (DSL):

- The DSL takes the lead for safeguarding and online safety, which includes overseeing and acting on:
- Filtering and monitoring reports
- Safeguarding concerns
- Checks to filtering and monitoring systems
- Takes day to day responsibility for online safety.
- Acts as the named point of contact on all online safety issues and liaises with other members of staff or other agencies, as appropriate.
- Facilitates training and advice for all staff, keeping colleagues informed of current research, legislation and trends regarding online safety and communicating this to the school community, as appropriate.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident.
- Monitors pupil internet usage, acting where required.
- Maintains the online safety incident log and record of actions taken and reviews the log periodically to identify gaps and trends.
- Reports regularly to the Headteacher and WSLT on the incident log, internet monitoring, current issues, developments in legislation etc.

The Director of Academic Enrichment and Communication (in conjunction with the DSL):

- Promotes an awareness of and commitment to online safety throughout the school community.
- Keeps the online safety component of the curriculum under review, to ensure that it remains up to date and relevant to pupils.

The Systems and Network Manager in conjunction with IT Service Providers:

- Maintaining filtering and monitoring systems
- Providing filtering and monitoring reports
- Completing actions following concerns or checks on systems

Director of IT, Systems Innovation and Digital Strategy and the DSL in conjunction with IT Service Providers:

- Procurement of systems, ensuring that the organisation acquires the necessary hardware and software to support its operations efficiently.
- Identifies potential risks that could impact the organisation's projects or operations, helping to develop strategies for mitigation.
- Carries out reviews of products and processes to assess their performance and compliance with established standards, facilitating continuous improvement.
- Routinely perform checks on the system to monitor its health, security, and performance, ensuring the organisation's digital infrastructure remains stable and secure.

Staff managing the technical environment:

- Apply appropriate technical and procedural controls to ensure that the school's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Keep up to date with the school's online safety policy and technical information to carry out their online safety role effectively and to inform and update others as relevant.
- Provide technical support to the DSL and leadership team in the implementation of online safety procedures.
- Ensure that the school's filtering policy is applied and updated on a regular basis and oversees the school's monitoring system.
- Report any filtering breaches or other online safety issues to the DSL, Head, and other bodies, as appropriate.
- Ensure that any safeguarding concerns are reported to the DSL, in accordance with the school's safeguarding procedures.

All school staff:

- Read, adhere to and help promote the E-Safety policy, Acceptable Use Agreements and other relevant school policies and guidance.
- Take responsibility for the security of school systems and the data they use or have access to.
- Model safe, responsible, and professional behaviours in their own use of technology.
- Embed online safety in their teaching and other school activities.
- Supervise, guide, and monitor pupils carefully when engaged in activities involving online technology (including extra-curricular and extended school activities if relevant).
- Have an up-to-date awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by reporting to the DSL.
- Know when and how to escalate online safety issues.
- Take personal responsibility for professional development in this area.

Pupils (at a level that is appropriate to their individual age, ability, and vulnerabilities):

- Engage in age-appropriate online safety education opportunities.
- Read and adhere to the school Acceptable Use Agreements.
- Respect the feelings and rights of others both on and offline, in and out of school.
- Take responsibility for keeping themselves and others safe online.

- Report to a trusted adult if there is a concern online.

Parents and carers:

- Read the school Acceptable Use Agreements and encourage their children to adhere to them.
- Support the school in online safety approaches by discussing online safety issues with their children and reinforcing appropriate, safe online behaviours at home.
- Model safe and appropriate use of technology and social media, including seeking permission before taking and sharing digital images of pupils other than their own children.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Use school systems, such as learning platforms, and other network resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

External groups:

- Any external individual/organisation must sign an Acceptable Use Agreement prior to being given individual access to the school network.

Appendix 2: Safer Use of Technology

Classroom Use

- The school uses a wide range of technology. This includes access to: Computers, laptops, and other digital devices
    - Internet which may include search engines and educational websites
    - Learning platforms
    - Cloud services and storage
    - Email, messaging, and video conferencing
    - Games consoles and other games-based technologies
    - Digital cameras, web cams and video cameras
    - Virtual reality headsets
- Supervision of pupils will be appropriate to their age and ability.
- All devices should be used in accordance with the school's AUAs and with appropriate safety and security measures in place.
- Members of staff should always check websites thoroughly, and tools and apps for suitability before use in the classroom or recommending for use at home.
- Staff and pupils should consider copyright law before using internet-derived materials by staff (and pupils should, where appropriate, comply with license terms and/or acknowledge the source of information).

Filtering and Monitoring

System logs from the software used for filtering and monitoring can be accessed, assessed and addressed by the DSL. Concerns identified will be managed according to the nature of the issue.

- The DSL works closely together with the IT team and IT service providers to meet the needs of the school.
- Service providers have given extensive training for the introduction of the systems and provide ongoing support as required.
- Any reported concerns and their outcomes are stored in a folder in the DSLs office. The information documented addresses:
    - When the checks took place
    - The person who performed the check
    - What was tested or checked
    - Resulting actions
- All buildings within Edgbaston High School are centrally provided with their data connections via a dedicated network. All incoming data is screened by an application that provides real-time filtering and protects both networks and users from internet threats. It prevents a wide range of unwelcome material and malware from being available in schools while at the same time allowing access to material of educational value.
- The policy determining filtering is managed centrally by the Network and Systems Manager, with different levels of permissions being applied depending on age group or user permission.
- The system logs all internet access on Edgbaston High School devices, and these logs can be accessed by the DSL for monitoring purposes. Flagged terms will also trigger alerts which the DSL may investigate. Concerns identified will be managed according to the nature of the issue.
- There is also a centrally managed process for scanning email messages between staff and students for inappropriate language and behaviour. If there is an issue the HR and Compliance Officer will be alerted and the matter taken up with the school. Email traffic between pupils is not scanned as a matter of course, but if concerns about contacts between pupils are raised, then a record of messages may be retrieved.

- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard pupils: effective classroom management and regular education about safe and responsible use is essential.
- All users are informed that use of school systems is monitored and that all monitoring is in line with data protection, human rights, and privacy legislation.

Filtering

Here are the key features of the software that is used for filtering the network:

- Lightspeed Relay is a comprehensive education technology platform designed to enhance online learning and provide a safe and effective digital learning environment for students and teachers.
- Content Filtering: Filters inappropriate content to ensure a safe online learning environment and blocks access to websites and resources that are not suitable for educational purposes.
- Classroom Management: Enables the school to control and limit access to specific websites or applications during class.
- Internet Usage Reporting: Provides detailed reports on students' internet usage and online behaviour.
- Remote Learning Support: Ensures students can safety access educational resources while learning from home.

Dealing with Filtering Breaches

The school has a clear procedure for reporting filtering breaches:

- If pupils discover unsuitable sites, they will be required to alert a member of staff immediately.
- The member of staff will report the concern (including the URL of the site if possible) to the DSL.
- The breach will be recorded and escalated as appropriate.
- Any material that the school believes is illegal will be reported immediately to the appropriate agencies, such as Internet Watch Foundation (IWF), the Police or Child Exploitation and Online Protection (CEOP).

Monitoring

Here are the key features of the software that is used for monitoring the network:

- Lightspeed Monitor - Managed Service is a real-time digital monitoring solution that offers a 24/7/365 human moderated service. A highly trained team monitor alerts and will notify the DSL of risks appropriate to their grade, meaning you can concentrate on providing support to the pupils in your care.
- Text analysis: Captures text input via the keyboard, whether online or offline, allowing you to monitor activity within encrypted sites and apps.
- 24/7/365 human moderation: Content is reviewed by a team of moderators around the clock to analyse instances and alert Safeguarding Officers of any high-risk incidents.
- Smart profiling: Builds an up to the minute profile of activity per individual, allowing the risk profile and context of a situation to be accurately analysed.
- Image capture: Screen capture functionality sits within the solution, allowing any online and offline incidents that require investigation to be screen grabbed for later review or evidence.
- Alerts and notifications: Alerts are based upon specific categories that are identified as serious incidents and will be sent to your Designated Safeguarding Lead.

Managing Personal Data Online

Personal data will be recorded, processed, transferred, and made available online in accordance with the *General Data Protection Regulations*. Full information can be found in the school's GDPR and Data Protection Policy.

Use at Home: Internet Access During Extended Holidays

- Internet Access Restriction – During long holiday periods (Summer, Christmas, and Easter), students' access to the school's internet network will be disabled on their iPad. This includes all school-managed devices and accounts that are linked to the school's online resources.
- Rationale for Restriction: The decision to restrict access during extended breaks is based on the following considerations:
    - To mitigate any potential cyber risks, including online bullying, inappropriate content, or security threats, when students are not under the direct supervision of the school's e-safety protocols.
    - To encourage responsible internet use and create a balance between online and offline activities.
- Access to Resources via RMUnify: Despite the restriction on general internet access on their school iPad, students will still have full access to their educational resources and schoolwork through RMUnify, allowing them to continue their studies and access necessary materials from home on their personal devices. This ensures that students can stay on track with their learning and assignments during holiday periods.
- Exceptions: In specific circumstances, such as revision or coursework requirements, limited access to other online resources may be granted on a case-by-case basis, subject to approval by school staff. These requests
- Parental Involvement: Parents and guardians will be informed of this policy and encouraged to take an active role in supervising their child's internet usage at home on personal devices during these holiday periods.

Appendix 3: Social Media Rules

These rules specifically cover the use of social media accounts set up in the school's name. Any social media account set up in the name of the school is covered by and must adhere to these rules. Social media use is mentioned in several other policies, in most circumstances other policies cover the personal use of social media.

Social Media in other policies.

- Acceptable Use Policy
- Data Protection Policy and GDPR notice
- Safeguarding Children Policy
- Employee Handbook

For the purpose of these rules an image is defined as any content, digital or otherwise, that shows a visual representation of a person, this definition includes, but is not limited to, photographs and video recordings.

We want to ensure that the personal data of all staff and students are kept safe, that school social media is used responsibly and that the school adheres to all legislative guidance

Social media can be an excellent marketing tool and it can be a great way to celebrate the achievements of the school and its students. However, everyone involved needs to be aware that placing any identifying information in the public domain has risks. Parents also need to understand these risks to give properly considered consent.

The most highly publicised and worrying risk is that a child who appears on social media may become of interest to a predatory sex offender. Locating people through the internet has become extremely easy, using widely available software, so if there is a picture and the name of the school and the name of a child it could be quite easy to find out the address of the child and even work out their most likely route to school.
There are also other specific groups of children and families whose safety could be put at risk if identified, e.g. looked after children.

Any image or other personal information, once posted online, can be copied, or shared by anyone and will stay online forever. There is also the concern that images of children may be copied directly from social media and then manipulated or changed by another person. To limit these potential risks the school must take appropriate steps to safeguard children.

Roles and Responsibilities

The *Headteacher and Designated Safeguarding Lead (DSL)* will be responsible for the implementation of social media governance and guidance.

The *Designated Safeguarding Lead* will ensure the social media guidance kept up to date and that staff using school social media have the necessary training.

The *Head of Marketing and Communications* will have access to any and all social media accounts set up in the school's name and will ensure the content posted adheres to this policy.

The *HR and Compliance Officer* who is responsible for Data Protection is must ensure the acceptable and safe storage of all images within the school.

Any member of staff who takes images or records videos for social media use and any staff who has access to post or add content of any kind to a social media account set up in the name of the school should read, understand, and follow the rules set out here.

Any breach of these rules may result in disciplinary action. Any member of staff suspected of breaching these rules will be required to cooperate with an investigation, which may involve accessing relevant passwords and login details. This would be in accordance with an employee's legal rights.

These rules are not intended to restrict all employee activity on social media. However, school representatives are asked to exercise caution and professional judgement about what they use it for, who they communicate with and the subject matter they post and interact with.

Official use of Images/ Videos of Children by the School

When taking images, staff should use school devices to take pictures. Staff should ensure that when taking images, only students with consent should be in the image. Staff should ensure that pupils are aware when images are being taken of them, this is for the safety of the pupils and the staff taking the images.

Care should be taken when taking images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

At school events such as school music and theatre productions, sports day, school prom and school parties, images should only be taken by members of staff selected to be the official photographers. Other staff members, volunteers or temporary staff members helping to run an event should not take photos or videos.

EYFS staff should be aware that DFE have stated that use of mobile phones and cameras in EYFS settings should be restricted. This is also covered in the school's safeguarding policy.

Any staff who use a personal device to access school storage should ensure that they have read and understood the Staff Handbook and E-Safety Policy covering staff use of personal devices. Any images accidentally taken using a personal camera must be deleted immediately/ as soon as the staff member becomes aware of the mistake. Steps should be taken to ensure the images have not been backed up onto personal cloud storage automatically and should be deleted immediately if this has happened.

Storage of Images

All images taken by the school will be stored in a safe and responsible manner that adheres to data protection principles.

Any staff who use a personal device to access school storage should ensure that they have read and understood the Staff Handbook & E-Safety Policy section that covers staff use of personal devices.

Once a student has left the school their image should not be used on social media unless the former student is contacted (or the former student's parents if the former student is still a child) and written consent is given.

Posting Content on Social Media

All staff must be aware that when content, including images, is uploaded to social media then the user agrees to the terms and conditions of that social media. For many social media websites this would mean that by uploading any images or videos the school is granting the site a license to copy, modify and use the images. This means that the school no longer "owns" the content, and it can be used without the school's consent or knowledge. To adhere to GDPR the Data Controller should undertake a risk assessment on any website or app that is used to share content, to identify possible dangers and

what actions may be taken by the school to limit any concerns.

The school should keep track of who has access to public facing social media accounts set up in the school's name, everyone who has access should receive adequate training on the safe and responsible use of social media. Public facing social media accounts will be managed by the *Head of Marketing and Communications*.

Specific guidance on social media posts:

- Any social media post created by an account that has been set up in the school's name should include as few personal details as possible.
- For every post staff should consider whether it is necessary to include the chosen level of detail; could detail be minimised further.
- The full name (first name and surname) of a child or adult should never be used in a post that
- contains an image.
- If the full name (first name and surname) of a child or adult must be used, then it must be done so without an image.
- If a photograph is of an individual child, then that child's first name should not be used.
- If a child has left the school their personal details, including images, should not be used in any new social media post, unless the school has gained written consent to continue using them.
- Personal contact details such as email, postal address and telephone numbers should not be used in any post at any time.
- If the school has a specific reason for breaching any of these guidelines in a specific post, they should ask for specific written consent to do so for that post only. Consent should come from parents if the child is under 12. If the child is 12 or over consent should come from parents and the child in question.

Consent

An image of a person is considered personal data and it is a requirement that written consent is obtained from the parent/ carer of a young child or young person under the age of 12 (or from him or herself if deemed to be competent to make such judgements from 12 years old as suggested by the Information Commissioner) for any photographs or video recordings.

The school will get general consent for the use of images when students join the school. Parents / carers will be made aware, prior to giving consent for images to be taken, that their child's image may be posted on social media.

Verbal consent must not be accepted under any circumstances. If it is not possible to obtain prior written consent, then images must not be taken involving the child or young person concerned.

The parent / carer has the right to refuse or withdraw consent at any time. Any images of a child whose parents have refused or withdrawn consent, must be destroyed.

If two parents disagree over consent for their child to appear in images, the school should treat this as though no consent has been given.

Consent should also be obtained from any staff member who appears in an image to be posted on social media.

Contact with students on social media Communication between children and adults should always remain professional. The school should never use school social media accounts to add or follow students. The school should never build or pursue relationships with children online, even if the child has left the school.

The school should never use the private messaging services linked to social media accounts to contact

any staff, student, parent, or family member of a student. Contacting anyone digitally should always be done through official channels, such as official school email accounts.

If a request is received from a child to add or follow school social media accounts this may be accepted. All children should be educated on the risks of social media.

Staff who have access to school social media accounts should ensure that all communications are transparent and open to scrutiny.

Use of images of Children by the Press

Occasionally images and personal details of students may be released to the press. It should be noted that the press enjoys special rights under the Data Protection Act, which permit them to publish material for journalistic purposes. In every case consent should be requested from parents before releasing any personal details to the press. Where students are over 12 years of age the student should also be asked to give consent for their personal details to be given to the press.

Liking, sharing, and retweeting.

Staff should ensure that any post created by any other account that is linked to the school social media account via liking, sharing, retweeting or any other method that allows direct connection between the school and that post, is also in line with this policy. Staff using the school social media account should not like, share, or retweet any post from any other account if it contains too many personal details about students or staff. For guidelines about what constitutes too much personal detail see the guidelines in the section. above.

Raising Concerns

If any member of staff has a concern about any post or content on any of the school social media accounts, they should raise it with the Head of Marketing and Communications and the Designated Safeguarding Lead.

If a child or parent makes a complaint to you, please forward this to the Head of Marketing and Communications and the Designated Safeguarding Lead.

Appendix 4: Use of Personal Devices and Mobile Phones

The school recognises that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff, and parents/carers, but technologies need to be used safely and appropriately within school.

Expectations

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies, including, but not limited to: Anti-Bullying, Behaviour, and Safeguarding and Child Protection.
- Electronic devices of any kind that are brought onto site are the responsibility of the user at all times. The school accepts no responsibilities for the loss, theft, damage, or breach of security of such items on school premises.
- Mobile phones are only permitted to be used by Sixth Form Students, in the Sixth Form Centre. All other students should use reception to contact home or use their mobile phone with explicit permission from a member of staff.
- The sending of abusive or inappropriate messages/content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt according to the behaviour policy.
- All members of the community are advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school behaviour or Safeguarding and Child Protection policies.

Staff Use of Personal Devices and Mobile Phones

- Members of staff will ensure that the use of personal phones and devices takes place in accordance with the law, as well as relevant school policy and procedures, such as: Confidentiality, Safeguarding and Child Protection, Data Security and Acceptable Use Agreements.
- Images of pupils must not be stored on personal devices. Any image taken on personal devices must be transferred to the school system as soon as reasonably possible and the personal copy permanently removed. Any copy backed up to cloud-based service must be removed.
- Throughout the setting all persons in the EYFS are required to adhere to the ICT Acceptable Use Agreement on the use of mobile phones and cameras: that is, that images of pupils may not be stored on personal devices. Any images taken on personal devices will be transferred to the school system as soon as reasonably possible and the personal copy permanently removed.

Pupils' Use of Personal Devices and Mobile Phones

- Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
- Pupil's mobile phones are expected to be kept in their Yondr pouch during the school day. For Sixth Form students they should keep them safely about their person.
- If a pupil needs to contact her parents or carers, they will be allowed to use their mobile phone or a school phone, as long as they have permission from a member of school staff.
- Parents are advised to contact their child via the school reception during school hours
- Mobile phones will not be used by pupils during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- Mobile phones and personal devices (such as smart watches) must not be taken into examinations. Pupils found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the pupil's grade in that examination, or all examinations being nullified.

- If a pupil breaches the school policy, the phone or device will be confiscated and will be held in a secure place
    - Searches for and of mobile phone or personal devices will only be carried out in accordance with the relevant government guidance.
    - Schools are not required to inform parents before a search takes place or to seek consent for a search for a prohibited item, or item which a member of staff reasonably suspects has been or is likely to be used to commit an offence or to cause personal injury or damage to the property of any person.
    - Where the person conducting the search finds an electronic device that is prohibited by the school rules or that they reasonably suspect has been, or is likely to be, used to commit an offence or cause personal injury or damage to property, they may examine any data or files on the device where there is a good reason to do so. They may also delete data or files if they think there is a good reason to do so, unless they are going to give the device to the police.
    - If there is a suspicion that material on a pupil's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.
    - The confiscation and searching of a phone or other digital device will normally be carried out in consultation with a senior member of staff.

Visitors' Use of Personal Devices and Mobile Phones

- Parents, carers, and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with the school's Acceptable use Agreement and other associated policies, such as Anti-Bullying and Safeguarding and Child Protection policies
- The school will ensure appropriate signage and information is provided to inform parents, carers, and visitors of expectations of use.
- Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL of any breaches of school policy.

Appendix 5: Useful links and sources of advice

Guidance and resources

- https://www.safeguardinginschools.eo.uk/
- Indecent images of children: guidance for young people
- Cyberbullying: understand, prevent and respond (Childnet)

National Organisations

- Action Fraud: www.actionfraud.police.uk
- CEOP:
    - www.thinkuknow.co.uk
    - www.ceop.police.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithful! Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
    - Childline: www.childline.org.uk
    - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
    - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
    - Telephone helpline: 0844 3814772
- 360 Safe Self-Review tool for schools: www.360safe.org.uk

EDGBASTON HIGH SCHOOL

Hardware Agreement for Staff

Staff Name: _____ Date: _____

Laptop Name: _____ iPad Name: _____

Laptop Serial No: _____ iPad Serial No: _____

Equipment

On the above date I acknowledged receipt of the following from Edgbaston High School for Girls (tick as applicable):

- ☐ Laptop and charger
- ☐ Apple iPad
- ☐ Apple iPad plug and charger lead
- ☐ iPad Case
- ☐ Kaligo Stylus
- ☐ Kaligo Stylus charger lead

Reporting Loss or Damage

Any damage or loss of items must be reported to the IT technicians immediately, where the damage or loss will be assessed and reported to the Director of Finance in serious cases.

Insurance

School insurance covers the equipment while it is away from the school in my custody, against non-culpable loss or damage. However, I am responsible for all culpable damage to the equipment.

Culpable damage is damage which I can be held liable because of insufficient care for the equipment. Examples include:

I am responsible:

- if the equipment is stolen from the interior of the car, wherever it may be parked;
- If the equipment is lost outside Edgbaston High School;
- If the equipment is left in a public place.

I am not responsible for:

- accidental damage to the equipment;
- damage to the equipment or if the equipment is stolen while it is left unattended during the school day or overnight in my classroom, the staff room or an office where reasonable care has been taken.

Access, Software and Updates

I shall use the equipment and the software only in connection with my work at Edgbaston High School and shall not permit any other person to possess or use the equipment or software that is installed on these devices.

I shall not sell, lease or otherwise grant anyone rights to the equipment or the software.

I agree to keep up to date the install virus protection software, network hot fixes and network updates by connecting the equipment to the school network at least once every week.

Departmental Equipment

If the equipment is allocated to a department, the Head of Department is responsible for maintaining a written record of the days and times when members of the department take the equipment out of school.

Equipment Returns

All staff are expected to return all of the original items to EHS upon request. This is most likely to happen either if an update is available or at the termination of your employment contract at EHS.

Failure to return the original item will result in the full charge for the original item being deducted from your salary. Alternative purchases to the original items will not be accepted. The amount charged will reflect the cost of a brand-new replacement item directly from the manufacturer e.g. Apple. If the items are found and returned to school the same amount will be refunded.

I have read, understand and agree to abide by the terms of the Hardware Agreement for Staff:

Name: _____

Signed: _____

Date: _____

EDGBASTON HIGH SCHOOL

Staff/Volunteers/Governors Acceptable ICT Use Agreement

This agreement applies to all adult users of the Edgbaston High School system including, but not limited to, staff, volunteers, peripatetic teachers and governors. It is expected that you use the ICT facilities sensibly, professionally, lawfully, consistent with your duties, with respect for your colleagues and in accordance with this agreement.

It is important that you read this agreement carefully. If there is anything that you do not understand, please discuss it with the Headteacher or the Director of Systems Innovation. Once you have read and understood this agreement thoroughly, you should sign this document, retain a copy for your own records and return the original to the ICT team, who will keep a record for the HR and Compliance Officer.

This should be read in conjunction with the Student Acceptable ICT Use Agreement - all adult users take responsibility for ensuring they enforce this agreement with pupils within their role in school.

Electronic information can be produced in court in the same way as oral or written statements. The school has an obligation to monitor the use of the internet and e-mail services provided in line with The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. Traffic data and usage information may be recorded and may be used in disciplinary procedures if necessary. The school reserve the right to disclose any information they deem necessary to satisfy any applicable law, regulation, legal process or governmental request. If there is any evidence that this agreement is being abused by individuals, we reserve the right to withdraw from employees the facility to view, send and receive electronic communications or to access the internet.

All information relating to our students, parents and staff is personal. You must treat all school information with the utmost care whether held on paper or electronically. Official school systems must be used at all times.

Use of the Network

Staff use of the network, including Internet access, is monitored by Lightspeed. This software monitors all keystrokes and takes screenshots when potentially inappropriate or harmful material is detected. If an unacceptable word or phrase is used the Designated Safeguarding Lead is notified by the software. Any concerns are reported to the Headteacher. If staff accidentally access inappropriate materials, they should immediately inform the Headteacher.

There is a forced change for passwords and these 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, ensuring memory sticks are password protected.

Use of the Internet

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. This is against Part 2 of the Teacher's Professional Standards. Examples might include pornography, hate material and material which others may find offensive such as sexist or racist material.

When entering an internet site, always read and comply with the terms and conditions governing its use. Be aware at all times that when visiting an internet site, the unique address for the computer you are using (the IP address) can be logged by the site you visit, thus identifying the school. For your information, the following activities are criminal offences under the Computer Misuse Act 1990:

- Unauthorised access to computer material e.g. hacking;
- Unauthorised modification of computer material; and
- Unauthorised access with intent to commit/facilitate the commission of further offences.

In line with this policy, the following statements apply:

- If you download any image, text or material check if it is copyright protected. If it is, then follow the school procedure for using copyright material.
- Do not download any image, text or material which is inappropriate or likely to cause offence. If this happens accidentally report it to a senior member of staff.
- If you want to download any software, first seek permission from the Headteacher and/or Network and Systems Manager. They should check that the source is safe and appropriately licensed.
- If you are involved in creating, amending, or deleting web pages or content on the web site, such actions should be consistent with your responsibilities and be in the best interests of the school.

You should not:

- Introduce packet-sniffing software (e.g. software which is used to intercept data on a network) or password detecting software
- Seek to gain access to restricted areas of the network
- Knowingly seek to access data which you are not authorised to view
- Introduce any form of computer viruses
- Carry out other hacking activities

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

Email

Care must be taken when using e-mail as a means of communication as all expressions of fact, intention or opinion may implicate you and/or the school.

Users are expected to use the school email system Outlook/Office 365 for school business and to communicate responsibly. They should add a disclaimer and signature to emails which are sent externally. They should not use the school email system for personal business.

Internet and e-mail access is intended to be used for school business or professional development. Any personal use is subject to the same terms and conditions and should be with the agreement of your Headteacher. Your privacy and autonomy in your business communications will be respected. However, in certain circumstances it may be necessary to access and record your communications for the school's business purposes which include the following:

- Providing evidence of business transactions

- Making sure the schools business procedures are adhered to
- Training and monitoring standards of service
- Preventing or detecting unauthorised use of the communications systems or criminal activities
- Maintain the effective operation of communication systems

In line with this policy the following statements apply:

- You should agree with recipients that the use of e-mail is an acceptable form of communication. If the material is confidential, privileged or sensitive you should be aware that un-encrypted e-mail is not secure.
- Do not send sensitive personal data via email unless you are using a secure site or password protected documents via OneDrive. It is good practice to indicate that the email is 'Confidential' in the subject line.
- Copies of emails with any attachments sent to or received from parents should be saved in a suitable secure directory.
- Do not impersonate any other person when using e-mail or amend any messages received.
- Sending defamatory, sexist or racist jokes or other unsuitable material via the internet or email system is grounds for an action for defamation, harassment or incitement to racial hatred in the same way as making such comments verbally or in writing.
- It is good practice to re-read e-mail before sending them as external e-mail cannot be retrieved once they have been sent.
- If the email is personal, it is good practice to use the word 'personal' in the subject header and the footer text should indicate if it is a personal email the school does not accept responsibility for any agreement the user may be entering into.
- Internet and e-mail access is intended to be used for school business or professional development, any personal use is subject to the same terms and conditions and should be with the agreement of your Headteacher.
- All aspects of communication are protected by intellectual property rights which might be infringed by copying. Downloading, copying, possessing, and distributing material from the internet may be an infringement of copyright or other intellectual property rights.

Social networking

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

The use of social networking sites for business and personal use is increasing. Access to social networking sites is blocked on the school systems. However, the school can manage access by un-filtering specific sites as internet usage is still monitored.

School staff may need to request access to social networking sites for several reasons including:

- Advertising the school or managing an 'official' school presence,
- For monitoring and viewing activities on other sites
- For communication with specific groups of adult users e.g. a parent group.
- Social networking applications include but are not limited to: o Biogs
- Any online discussion forums, including professional forums
- Collaborative spaces such as Wikipedia
- Media sharing services e.g. YouTube, Flicker
- 'Microblogging' applications e.g. Twitter

When using school approved social networking sites the following statements apply:

- School equipment should not be used for any personal social networking use.

- Staff must not accept friendships from students. The legal age for students to register with a social networking site is usually 13 years; be aware that some users may be 13 or younger but have indicated they are older.
- It is important to ensure that members of the public and other users know when a social networking application is being used for official school business. Staff must use only their school email address or other school approved email mechanism and ensure all contributions are professional and uphold the reputation of the school.
- Social networking applications should not be used to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claims for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the school into disrepute.
- Postings should not be critical or abusive towards the school, staff students, or parents or used to place a student, student, or vulnerable adult at risk of harm.
- The social networking site should not be used for the promotion of personal financial interests, commercial ventures, or personal campaigns or in an abusive or hateful way.
- Ensure that the appropriate privacy levels are set. Consider the privacy and safety settings available across all aspects of the service - including photos, blog entries and image galleries. Failing to set appropriate privacy levels could result in messages which are defamatory, libellous, or obscene appearing on your profile before you have chance to remove them.
- It should not breach the schools Information Security Policy.

Data Protection

The processing of personal data is governed by the Data Protection Act 2018. Schools are defined in law as separate legal entities for the purposes of complying with the Data Protection Act. Therefore, it is the responsibility of the school to ensure that compliance is achieved.

As an employee, you should exercise due care when collecting, processing, or disclosing any personal data and only process personal data on behalf of Edgbaston High School. The main advantage of the internet and e-mail is that they provide routes to access and disseminate information.

Through your work personal data will come into your knowledge, possession, or control. In relation to such personal data whether you are working at Edgbaston High School's premises or working remotely you must:

- Keep the data private and confidential and you must not disclose information to any other person unless authorised to do so. If in doubt, ask the Headteacher.
- Familiarise yourself with the provisions of the Data Protection Act 2018 and comply with its provisions
- Familiarise yourself with all appropriate school Policies and Procedures
- Not make personal or other inappropriate remarks about staff, students, parents or colleagues on manual files or computer records. The individuals have the right to see all information the school holds on them subject to any exemptions that may apply.

If you make or encourage another person to make an unauthorised disclosure knowingly or recklessly you may be held criminally liable. I have read through and fully understand the terms of the policy. I also understand that Edgbaston High School may amend this policy from time to time and that I will be issued with an amended copy.

Failure to Follow Policy

Specific breach of this agreement might include deliberately accessing, printing, showing or transmitting inappropriate material within the school's network or via the Internet. There are sanctions for deliberate access to inappropriate materials by users according to the level of the offence.

Any inappropriate use of Edgbaston High School's internet and e-mail systems, whether under this agreement or otherwise, may lead to disciplinary action being taken against you under the appropriate disciplinary procedures which may include immediate suspension, which may lead to dismissal.

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

Name: _____

Signature: _____

Date: _____

EDGBASTON HIGH SCHOOL

Student iPad Acceptable Use and Returns Policy

Our 1:1 iPad programme equips students with a personal digital device, technology and resources for the modern classroom thus enabling independent learning, supporting high attainment levels and the development of students' study skills both in school and at home.

Equipment Issued to Students

Students at EHS are issued with the following equipment when they start in Senior School:

- Apple iPad
- Apple iPad plug and charger lead
- iPad Case
- Kaligo or Tucano Stylus
- Kaligo or Tucano Stylus charger lead

Students will have access to these facilities throughout their time in Senior School.

Equipment Returns

All students are expected to return all of the original items to EHS upon request. This is most likely to happen either at the end of a year if an update is available or at the end of the student's time at EHS.

Failure to return the original item will result in the charge for the original item being added to the termly or final invoice. Alternative purchases to the original items will not be accepted.

Any damage to items must be reported to the IT technicians immediately, where the damage will be assessed. Students are entitled to one iPad repair up to the value of £100 free of charge during their time at EHS where accidental damage has occurred. Screen repairs can be significantly higher than this amount. Payment for any further repairs will be decided on an individual basis.

Any lost items must also be reported to the IT technicians immediately. Whether the items are lost inside or outside school, the charge for the lost item will be added to the termly invoice. The amount charged will reflect the cost of a brand-new replacement item directly from Apple. If the items are found and returned to school the same amount will be refunded.

Acceptable Use

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 schoolwork, 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 or 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 Network Manager and Systems Manager or the 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.
- If an iPad is damaged it will be repaired on one occasion free of charge up to the value of £100.

Prohibited Uses (not exclusive):

- Accessing Inappropriate Materials - All material on the iPad must adhere to the ICT Responsible Use Policy. Users are not allowed 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.
- 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

The iPad Acceptable Use Policy Agreement

THIS WILL BE COMPLETED BY STUDENTS IN SCHOOL WHEN THEY RECEIVE THEIR DEVICE

Summary of Student Agreement for iPad Use:

- will take good care of my iPad.
- will never lend my iPad to others.
- will know where my iPad is at all times.
- will charge my iPad every night and not at school.
- will provide a pair of earphones for use in school.
- will keep food and drinks away from my iPad since they may cause damage to the device.
- will not disassemble any part of my iPad or attempt any repairs.
- will protect my iPad by only carrying it whilst it is in a case.
- will only use my iPad in ways that are appropriate.
- will only download free educational apps onto the iPad which have been allocated by the school.
- understand that my iPad is subject to inspection at any time without notice.
- will only photograph people with their permission.
- will only use the camera or the microphone when my teacher tells me to.
- 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.

Student Signature _____

Student Name _____

Student Form _____

Date _____

EDGBASTON HIGH SCHOOL

Student Acceptable Use ICT Agreement

The school has a range of computer systems and Internet access to assist learning. These rules will keep everyone safe. It is important that you read this agreement carefully. If there is anything that you do not understand, please ask a teacher or a remember of ICT staff.

This acceptable use agreement is intended to ensure:

- students are responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- school systems and users are protected from accidental or deliberate misuse that could put the security of the systems at risk.
- students agree to be responsible users of the school's ICT systems.

Acceptable Use Agreement

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.

Edgbaston High School and Parents

- ICT staff will monitor use of the network, Internet and email and ensure 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.

For my safety:

- I understand that the school may check my computer files and will monitor the Internet sites I visit.

Network

- Users will take responsibility for their use of the computer network and Internet
- The transfer of program files to or from the network is strictly forbidden.
- The school ICT systems may not be used for private, commercial or political purposes unless permission has been granted by staff.

For my safety:

- 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, without prior permission from ICT staff.

The Internet

- Users will stay away from inappropriate sites when using the Internet.
- If users mistakenly access inappropriate information on the Internet, they should immediately tell a teacher and must not show this or discuss this with others.

- 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.
- Any misuse will result in withdrawal of the privilege of using these.
- Users will never give out personal information or arrange to meet anyone you encounter on the Internet.

For my safety:

- I will only use social media sites with permission and at the times that are allowed.
- I will not access inappropriate materials such as pornographic, racist, or offensive material or use the school system for personal financial gain, gambling, political purposes or advertising.
- I will not play games on the Internet unless these have a significant educational value and a teacher has given permission.
- When using the internet including a 'chat room' facility, I will not give my name, school name or location, home address, telephone/ mobile number, photograph, respond to requests using text or even arrange to meet someone, unless my parent, carer or teacher has given permission.

Access

- Access to the school network and Internet is available from any network station during the normal school day and from home via the 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.

For my safety:

- I will not share my password with anyone or use anyone else's password. If I become aware of another individual's password, I will inform that person and a member of the school staff.
- I will use a 'strong' password e.g. one that contains letters (upper case and lower case), numbers and possibly symbols which I will change on a regular basis.

Security and Privacy

- Do not attempt to bypass security or attempt to alter settings in place on the computers.
- Anti-virus software is installed on every server and station and is updated regularly to prevent viruses. The computer network and devices are regularly scanned and if a threat is identified you should let your teacher know immediately.
- The use of memory sticks not allowed unless provided or password protected by the School and pupils must take responsibility for ensuring that the appropriate virus checks are in place on home devices.
- Mobile equipment such as laptops can be connected wirelessly. It is the pupil's responsibility to ensure that adequate virus checks are in place.

For my safety:

- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to 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 use school equipment properly and not interfere with the work or data of another student.
- Before I use or connect my own personal equipment (mobile phone, non-school laptop/tablet etc.) I will check with a member of staff to ensure this is allowed.
- I will only use my own personal devices (mobile phones/USB devices etc.) in school if I have

permission. I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.

Copyright and Permissions

- 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.

For my safety:

- I will not download or bring into school unauthorised programmes, including games and music, or run them on school computers, laptops, or iPads.
- I will always follow the 'terms and conditions' when using a site. I know content on the web is someone's property and I will ask a responsible adult if I want to use information, pictures, video, music or sound to ensure I do not break copyright law.
- I will think carefully about what I read on the Internet, question if it is from a reliable source before I use the information, crediting the source.
- I will not make audio or video recordings of another student or teacher without their permission.
- I will always check with a responsible adult before I share or publish created content of myself or others.

Electronic Communication

- You may only use the school Outlook email system for school business and may not use any other web- based email services (e.g. Hotmail, Gmail etc).
- 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 emails and chain emails are not allowed.
- The school email address cannot be used for political, commercial or private use.
- You must always treat others with respect. It is unacceptable to transmit offensive or harassing messages.

For my safety:

- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation 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 am responsible for all e-mail, chat, texts, biogs etc. that I post or send and will use language appropriate to the audience who may read them.
- I will be respectful in how I talk to and work with others online and never write or participate in online bullying.
- I will report any unpleasant material or messages sent to me. I understand my report will be confidential and may help protect other students and myself.
- I know that posting anonymous messages and forwarding chain letters is forbidden.
- Any files attached to an email will be appropriate to the body of the email and not include any inappropriate materials or anything that threatens the integrity of the school ICT system.

ICT Rooms, Printers and Workstations

- No food or drinks may be taken into the ICT Department or near any other computers around school.
- 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.

For my safety:

- I will immediately report any damage or faults involving equipment or software.

Responsibility

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

- I understand the school has the right to take action against me if I am involved in incidents of inappropriate behaviour both in and out of school (examples would be online-bullying or inappropriate use of images or personal information).
- I understand that if I fail to comply with this acceptable use agreement, I may be subject to disciplinary action. This could include loss of access to the school network/internet, detentions, suspensions, contact with parents and involvement of the police in the event of illegal activities.
- I know that anything I share online will be monitored.
- I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

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.

I am aware of the CEOP report button and know when to use it.

The Click CEOP button is an asset of the National Crime Agency's CEOP Command. The CEOP Command works to protect children from the harm of sexual abuse and exploitation both online and offline.
The Click CEOP button provides a gateway to the CEOP Safety Centre offering:

- Advice on a range of online safety issues, such as hacking and cyberbullying;
- Signposting to NCA-CEOP partners offering help and support on issues outside of CEOP's remit, such as Childline and BeatBullying;
- Reporting of suspected or known child sex offender activity directly to CEOP for investigation.

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

Student Signature: _____

Student Name _____

Date _____