KING HENRY VIII
SCHOOL

Online Safety Policy

Name of policy	Date reviewed	By whom	Next review	Responsibility
Online Safety Policy	November 2022	Dr M Cuthbert Deputy Head	Annually November 2023	Dr M Cuthbert
Update New - Appendix 2	March 2024	Head	September 2024	Dr M Cuthbert

Table of Contents

1. Policy Introduction and Aims

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. In order 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 purpose of the online safety policy is to:

- Safeguard and protect all members of the school's community online;
- Identify approaches to educate and raise awareness of online safety throughout the community;
- Enable all staff to work safely and responsibly to model positive behaviour online and to manage professional standards and practice when using technology;
- Identify clear procedures to use when responding to online safety concerns.

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.

2. Policy Scope

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.

3. Links with other policies and practices

This policy links with several other policies, including:

- Data Protection Policy
- Safeguarding and Child Protection Policy
- Staff Code of Conduct
- Acceptable Use Agreements for staff and pupils
- School Behaviour Policy
- Anti-Bullying Policy

4. Roles and Responsibilities

All members of the community have important roles and responsibilities to play regarding online safety:

4.1 Governors:

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy by reviewing e-safety incidents and monitoring reports. Online safety falls within the remit the governor responsible for safeguarding. Governors will:

- Make sure an online safety policy is in place and is available to all stakeholders;
- Make sure that the DSL has been trained to a higher level of knowledge which is relevant to the school, up to date and progressive;
- Make sure that procedures for the safe use of ICT and the internet are in place and adhered to;
- Hold the Headteachers and staff accountable for online safety.

4.2 The Head:

- Has overall responsibility for online safety provision;
- Ensures that online safety is viewed as a safeguarding issue and that practice is in line with national recommendations and requirements;
- 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, local and national support;
- Receives regular reports from the DSL on online safety;
- Ensures that online safety practice is audited and evaluated regularly in order to identify strengths and areas for improvement.

4.3 The Designated Safeguarding Lead (DSL):

- Takes day to day responsibility for online safety;
- Promotes an awareness of and commitment to online safety throughout the school community;

- Acts as the named point of contact on all online safety issues, and liaises with other members of staff or other agencies, as appropriate;
- Keeps the online safety component of the curriculum under review, in order to ensure that it remains up to date and relevant to pupils;
- 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 Head and SLT on the incident log, internet monitoring, current issues, developments in legislation etc.

4.4 Network Manager/IT Team

- 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, while allowing learning opportunities to be maximised;
- Keep up to date with the school's online safety policy and technical information in order 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.

4.5 All School Staff:

- Read, adhere to, and help promote the online safety policy, acceptable use agreements and other relevant school policies and guidance;

- Model safe, responsible, and professional behaviours in their own use of technology;
- 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.

4.6 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.

4.7 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.

5. Education and Engagement

5.1 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 (PSHE), Relationships and Sex Education (RSE) 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 pupils 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 AUA and its implications, and reinforcing the principles;
- 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.

5.2 Training and Engagement with Staff

The school will:

- Provide and discuss the Online 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.

5.3 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 DSL In Touch Pastoral Letters and highlighting online safety at other events such as parent and setting the scene 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.

6. 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.

7. Safer Use of Technology

7.1 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 and messaging
  - Digital cameras, web cams and video cameras
- Supervision of pupils will be appropriate to their age and ability;
- All school-owned 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, 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 (and where appropriate comply with licence terms and/or acknowledge the source of information).

7.2 Filtering and Monitoring

- King Henry VIII School is provided with their data connections via a dedicated network. All incoming data are 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, with different levels being applied depending on age group;
- The system logs all internet access, 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;
- A member of the IT department has been trained to monitor online incidents within school. The details of these incidents are added to our Safeguarding Software, which the DSL will ten triage;
- Email traffic between pupils and staff is not scanned as a matter of course, but if concerns are raised, then a record of messages may be retrieved;
- All members of staff are however 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.

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).

7.3 Managing Personal Data Online

Personal data will be collected, processed, stored and transferred in accordance with the General Data Protection Regulations and the King Henry VIII School Privacy Notice. Full information can be found in the school's Data Protection Policy.

8. Social Media

8.1 Expectations

- The term social media includes (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and messaging services;
- All members of the school community are expected to engage in social media in a positive, safe and responsible manner, at all times.

8.2 Staff Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing sites is discussed with all members of staff as part of staff induction and is revisited and communicated via regular staff training opportunities;
- Safe and professional behaviour is outlined for all members of staff as part of the staff Code of Conduct and the Staff Acceptable Use Agreement.

8.3 Pupils' Personal Use of Social Media

- Safe and appropriate use of social media will be taught to pupils as part of online safety education, via age-appropriate sites and resources;
- The school is aware that many popular social media sites state that they are not for children under the age of 13. The school will not create accounts specifically for children under this age;
- The school will control pupil access to social media while using school-provided devices and systems on site;
- The use of social media by any pupil except in the Sixth Form during school hours for personal use is not permitted;
- Inappropriate or excessive use of social media during school hours or while using school devices may result in disciplinary or legal action and/or removal of internet facilities;

- Any concerns regarding pupils’ use of social media, both at home and at school, will be dealt with in accordance with existing school policies. Concerns will also be raised with parents/carers as appropriate, particularly when concerning underage use of social media sites or tools.

9. 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.

9.1 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 Discipline, 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 and Smart Watches not permitted to be used by pupils from the time they enter the school site in the morning to when they leave the school building at 4 pm, The use of mobile phones within school is seen as a safeguarding concern and if a student is found to be using one at an inappropriate time then they will incur a Level 4 Sanction (Tuesday Detention);
- Mobile phones may only be used during the school day by students in the Sixth Form or by other pupils under the direct supervision of a member of staff. These students are encouraged to connect to the school WiFi when using their devices in school;
- 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.

9.2 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 (other than a member of staff's own children) must not be stored on personal devices;
- Staff are encouraged to not use their mobile phones in the presence of pupils unless in an emergency situation or when needed to share travel and trip information.

9.3 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 personal devices and mobile phones are expected to be kept in a secure place, switched off, kept out of sight during the school day (except for Sixth Formers in the Sixth Form Centre);
- Sixth Former may use their phones in the Sixth Form centre;
- If a pupil needs to contact his/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 office during school hours;
- Mobile phones or personal devices 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 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 police will be informed 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.

9.4 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;
- Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL of any breaches of school policy.

10. 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), 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;
- 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.

10.1 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.

10.2 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 Head;
- Pupils and parents are informed of the school's complaints procedure.

11. Monitoring 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 the King Henry VIII 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.

12. Useful links and sources of advice

12.1 Guidance and resources

- Teaching Online Safety in School (DfE)
- Education for a Connected World (UKCIS)

- Sharing nudes and semi-nudes: advice for education settings working with children and young people (UKCIS)
- Indecent images of children: guidance for young people
- Cyberbullying: understand, prevent and respond (Childnet)
- Cyberbullying: advice for headteachers and school staff (DfE)

12.2 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 Faithfull 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 381 4772

Appendix 1: Acceptable Use Policy for Remote Learning – updated for camera use

Principles

- We are aiming to continue to provide an excellent education to all our students;
- Interacting with each other on-line is no different than interacting face-to-face: we are required to maintain the principles of respect, dignity, prudence, concern for and protection of others, and safety in all interactions.

General Conduct

- Students must conduct themselves in the same way they would in school;
- Language, both spoken and written, should remain appropriate and suitably academic;
- We continue to expect the highest standards of politeness and integrity from our students;
- We expect students to access their full curriculum as much as they are reasonably able to;
- We expect students to meet all deadlines set by staff for the submission of work unless affected by illness or other extenuating factors;
- Students must respect the privacy of others and so must not share photos, videos, contact details, or other information about members of the school community, even if the content is not shared publicly, without going through official channels and obtaining permission.

Conduct in 'Live' Lessons (Meetings)

- Meetings will only occur with a minimum of three people present, including at least one teacher;
- Students may join any Meeting occurring in their normal class Team;
- Students must leave a Meeting when instructed to do so;
- Staff will advise students of when Meetings will occur in advance, where possible this will be in a normal lesson slot;
- Students should only enable microphones with teacher permission;
- Students should be mindful of the appropriateness of possible background sound when using their microphone;
- Meeting text chats should only be used for learning conversations as directed by the teacher; these chats are logged within Teams.

Student Camera Use on Microsoft Teams

- Students must remember that they have agreed to follow our Acceptable Use Policy and should conduct themselves with the same standards of behaviour we expect in school;
- We expect them to adhere to the following guidelines for use of their camera:
    - Choose an appropriate location, not a bedroom, if possible;

- Choose a location where other people will not appear on camera without realising;
- Blur the background or add a false background using the video settings within Teams;
- If this is not possible, choose a location with a plain background;
- Be appropriately dressed at all times;
- Only turn on the camera if the teacher asks students to do so and only ever after the live lesson has started. Students will never be required to use their camera and should only do so when they feel comfortable;
- Be prepared to turn the camera off immediately if requested to do so;
- Do not use the camera as a way of communicating with others during lessons;
- The right to use a camera is a privilege we will grant in order to aid pupils' education and can be withdrawn at any time. Any misuse of a camera will be considered a serious breach of rules and will be sanctioned accordingly.

Use of Shared Resources

We expect that all resources shared by members of staff are only used as directed and, on the platforms, provided by King Henry VIII School. If resources are shared, including audio and video, students must not:

- take screenshots;
- share content outside of the Team;
- record any part of a lesson or video;
- post any content on to another site/platform;
- share any of the resources outside of the school.

Sanctions

- Teachers will report unacceptable behaviour to Heads of Year and Senior Staff;
- In the event of unacceptable conduct, we will continue to use a 'stepped approach' to sanctioning behaviour. This may include:
    - removing students from live Meetings;
    - limiting student contribution rights in Teams;
    - removing student access to live Meetings;
    - removing student access to any/all shared resource.

Appendix 2: Acceptable Use Policy for On-site Learning

ACCEPTABLE USE OF ICT POLICY (AUP)

Core Values:

Safety Responsibility Respect Honesty Integrity

POLICY AGREEMENT

Please read these statements and confirm your agreement:

1.1. Personal Safety

- I will keep my username and password safe and secure. I will not share it and will not write it down or store it where it is possible that someone may steal it.
- I will change my password at least once a term and will use a combination of 8 characters including capital and lowercase letters and numbers.
- I will not log on as anyone else; I will not use any other person's username or password.
- I will not disclose or share personal information about myself or others when online (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.). This does not apply to Sixth Form pupils who are registering with UCAS.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.
- I understand that the school will monitor my use of the systems, devices and digital communications and record and act upon anything they are concerned about.

NB

- **I understand how to manage my privacy settings and safety features of websites.**
- **I understand how to use or deactivate location settings or GPS on websites, apps or games.**
- **If I arrange to meet people offline that I have only communicated with online, I will do so in a public place and take an adult with me.**

1.2. Responsible Use

- I will not eat or drink in computer areas as spillages can cause serious damage to hardware.
- I understand that the school systems and devices are intended for educational use and that I will not use them for personal or recreational use, including OneDrive.
- I will not waste resources by printing unnecessary copies. I will check my work before printing. Wherever possible, I will use both sides of the sheet of paper, for copying or printing; print only the pages I need by using the 'Print Selection' function, and to reduce the number of pages printed, I will reduce margins, use the 'Print Preview' function before printing, use a small font size and use efficient fonts such as Times New Roman or Arial which use significantly less space.
- I will only print material related to school-based work or activities.

- I will not download or upload files that might take up internet capacity and prevent other users from being able to carry out their work.
- I will delete files from my area that I no longer require.
- I will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others.
- I will not attempt 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 not use school systems or devices for social networking, online gaming, online gambling, internet shopping, file sharing for non-educational purposes, or recreational video broadcasting (e.g. non-educational aspects of YouTube).
- 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.
- I will not open 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 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 unless for educational purposes.
- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will immediately report any damage or faults involving equipment or software however this may have happened.

1.3. Respectful Communication

- I will be polite and responsible when I communicate with others. I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions. I understand this includes all forms of electronic communication including email, social networking, blogging, gaming etc – whether at home or in school.
- I will not use inappropriate language when naming files or choosing passwords.
- I will only use my official school account to send and receive emails. This rule does not apply to Sixth Form pupils who use their personal emails for UCAS communication.
- I will not take or distribute images of anyone without their permission. I will not send Spam emails (chain, junk or bulk emails).

NB. We expect that you will uphold this standard of behaviour when you communicate with members of our community outside of school and act with respect, courtesy and integrity at all times.

1.4. Digital Honesty

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

- I should ensure that I have permission to use the original work of others in my own work.

- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

1.5. Sanctions

I understand that if I fail to comply with this Acceptable Use Policy Agreement (AUP) I will be subject to disciplinary action in accordance with the schools 'stepped approach to discipline' as set out in the School Code of Conduct and Behaviour Policy. This may include detentions, suspensions, fixed term or permanent exclusion, contact with parents and, in the event of illegal activities, involvement of the police and/or the Local Safeguarding Children's Board.

Signed by: **Endorsed by:**

____ ______________________________

Pupil name: **Parent name:**

____ ______________________________

Date:

____ ______________________________

END