Fairfield High School for Girls

Policy for E-Safety (Pupils, Parents and Carers)

Approved by:	Quality of Education Committee	**Date:** February 2024
Last reviewed:	September 2021	
Next review due by:	February 2025	
Person Responsible:	Deputy Headteacher and Senior Assistant Headteacher	

Aims

Fairfield High School aims to:

- have robust processes in place to ensure the online safety of pupils.
- deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology.
- establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

Scope

The school believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all pupils are protected from potential harm online.

The school:

- identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life;
- is aware that technology is a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse online as well as face-to-face;
- believes that pupils should be empowered to build resilience and to develop strategies to manage and respond to risk online.

This policy applies to all pupils, parents and carers. This policy applies to all access to the internet and use of technology, including personal devices, or where pupils have been provided with setting issued devices for use off-site, such as a work laptops.

Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

Teaching online safety in schools

Preventing and tackling bullying and cyber-bullying: advice for Headteachers and school staff

Relationships and sex education

Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so. The policy also considers the National Curriculum Computing Programmes of Study.

Monitoring and Review

Technology in this area evolves and changes rapidly; the school will review this policy at least annually. The policy will also be revised following any national or local policy requirements. We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied. To ensure they have oversight of online safety, the DSL, ICT strategy and safeguarding team will be informed of online safety concerns, as appropriate. The named Trustee for child protection and safeguarding including the full remit of online safety is Mrs Stafford. He will report on a regular basis to the Trust Board on online safety practice and incidents, including outcomes. Any issues identified via monitoring will be incorporated into our action planning.

Key Responsibilities of the Fairfield Community

The Board of Trustees

The Trust Board has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation. The Trust Board will coordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL).

The Headteacher

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

Pupils

Pupils are expected to:

- Engage in age appropriate online safety education opportunities;
- Read and adhere to the terms of the Acceptable Use Agreements;
- Respect the feelings and rights of others both on and offline;
- Take responsibility for keeping themselves and others safe online;
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

Parents/Carers

Parents/Carers are expected to:

- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2).
- **Read the acceptable use policies and encourage their children to adhere to them.**
- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the setting, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Use our 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.

Parents/Carers can seek further guidance on keeping children safe online from the following organisations and websites:

What are the issues? - UK Safer Internet Centre
Hot topics - Childnet International
Parent factsheet - Childnet International
Healthy relationships – Disrespect Nobody

Educating Pupils about Online Safety

The school will establish and embed an online safety curriculum to raise awareness and promote safe and responsible online behaviour at school and at home amongst pupils by:

- Ensuring education regarding safe and responsible use precedes internet access.
- Including online safety in Relationship, Social, Health and Economic (RSHE), Relationships and Sex Education (RSE) and computing programmes of study.
- Online safety is also to be covered in each year of the KS3 IT/Computing curriculum.
- Reinforcing online safety messages whenever technology or the internet is in use.
- 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.

The school will support pupils to read and understand the Acceptable Use Agreements in a way which suits their age and ability by:

- Displaying acceptable use posters in all rooms with internet access.
- Informing pupils that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
- Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

Vulnerable Pupils

The school recognises that some pupils are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.

- The school will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable pupils.
- When implementing an appropriate online safety policy and curriculum the school will seek input from specialist staff as appropriate, including the SENDCO, Designated Teacher for LAC and other appropriate staff.

Pupils will be taught about online safety as part of the Computing curriculum. In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy.

- Recognise inappropriate content, contact and conduct, and know how to report concerns.

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity.
- How to report a range of concerns.

By the **end of secondary school**, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online.
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online.
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them.
- What to do and where to get support to report material or manage issues online.
- The impact of viewing harmful content.
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners.
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties.
- How information and data is generated, collected, shared and used online.
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours.

The safe use of social media and the internet will also be covered in other subjects and through the pastoral structure where relevant.

The Computing curriculum 2023 - 2024:

- Y7 - Unit 1 - Using Computers Safely Effectively and Responsibly
- Y7 - Unit 2 - Managing Online Information
- Y7 - Unit 3 - Microbit Programming
- Y7 - Unit 4 - Understanding Computers
- Y7 - Unit 5 - Lego Coding Success
- Y8 - Unit 1 - Cyber Crime and Security
- Y8 - Unit 2 - Introduction to Python
- Y8 - Unit 3 - AWS GetIT
- Y8 - Unit 4 - Privacy and Security
- Y8 - Unit 5 - Spreadsheet Modelling
- Y9 - Unit 1 - Computational Thinking and Python
- Y9 - Unit 2 - AWS GetIT
- Y9 - Unit 3 - AI and Machine Learning
- Y9 - Unit 4 - Copyright and Plagiarism
- Y9 - Unit 5 - Data Science

KS4 Experience Time:

- IT and the world of work
- Thrive and Aspire Workshops

Educating Parents/Carers about Online Safety

The school will raise parents/carers awareness of internet safety in letters or other communications home, and in information via our website alongside access to the National Online Safety platform. Webinars and materials will be shared with parent/carer linking to key messages and any key items in the news.

- If parents/carers have any queries or concerns in relation to online safety or this policy, these should be raised in the first instance with the Headteacher and/or the DSL.

Reducing Online Risk

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

We 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 the setting 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.
- Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our computers or devices.

All members of the community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in our Acceptable Use Agreements and highlighted through a variety of education and training approaches.

Preventing and addressing cyber-bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim. The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Cyber-bullying will be actively discussed in both Computing lessons and Life Skills lessons. The school also sends information/leaflets on cyber-bullying to parents/carers so that they are aware of the signs, how to report it and how they can support children who may be affected. This is also covered in the National Online Safety resources.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school's Policy for Outstanding Conduct and Behaviour. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained. The DSL will consider whether the incident should be reported to the Police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Safer Use of Technology - Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so. When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the Senior Leadership Team to: retain it as evidence (of a criminal offence or a breach of school discipline), and/or report it to the Police.

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation. Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Classroom Use

Fairfield High School for Girls 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
- Email
- Digital cameras, web cams and video cameras
- All setting owned devices will be used in accordance with our Acceptable Use Agreements and with appropriate safety and security measures in place.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- We will ensure that the use of internet-derived materials, by staff and pupils complies with copyright law and acknowledge the source of information.
- Supervision of pupils will be appropriate to their age and ability.

Acceptable use of the internet in school

- Access to our devices and systems is granted via user accounts and records are maintained.
- All pupils will read and sign an Acceptable Use Agreement before being given access to our computer system, IT resources or internet.

- All pupils are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendix 1). Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.
- We will monitor the websites visited by pupils, to ensure they comply with the above.
- More information is set out in the acceptable use agreements in appendix 1.

Filtering and Monitoring

Filtering

- We use Smoothwall* which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
- The filtering system blocks all sites on the Internet Watch Foundation (IWF) list.
- We work with our broadband provider* and Smoothwall* to ensure that our filtering policy is continually reviewed.
- If pupils discover unsuitable sites, they will be required to report this immediately to a member of staff.
- The member of staff will report the concern (including the URL of the site if possible) to the DSL and ICT Manager.
- The breach will be recorded and escalated as appropriate.
- Parents/carers will be informed of deliberate filtering breaches involving their child.
- Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, Police or CEOP.

Monitoring

We will appropriately monitor internet use on all setting owned devices. This is achieved by:

- Use of our monitoring systems such as Smoothwall* and ESafe*.
- Reports are sent to the DSL and the Headteacher by ESafe to investigate.
- If a concern is identified via monitoring approaches we will:
    - Safeguarding team will respond in line with the Policy for Child Protection and Safeguarding.
    - All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.
- The DSL logs behaviour and safeguarding issues related to online safety.

Security and Management of Information Systems

We take appropriate steps to ensure the security of our information systems, including:

- Virus protection being updated regularly.
- The appropriate use of user logins and passwords to access our network.
- All users are expected to log off or lock their screens/devices if systems are unattended.

Password policy

- All pupils are provided with their own unique username and private passwords to access our systems; pupils are responsible for keeping their password private.

- We require all users to:
    - Always keep their password private;
    - Users must not share it with others or leave it where others can find it.
    - Not to login as another user at any time.

Pupil email

- Pupils will use provided email accounts for educational purposes. Pupils will sign an Acceptable Use Agreement and will receive education regarding safe and appropriate email etiquette.

TEAMS – the school learning platform for remote education

- Leaders and staff will regularly monitor the usage of TEAMS.
- All users will be mindful of copyright and will only upload appropriate content onto TEAMS.
- Any concerns about content on TEAMS will be dealt with in the following ways:
    - The user will be informed of material deemed to be inappropriate or offensive.
    - The user will remove the content.
    - If the user does not comply, the material will be removed by the site administrator.
    - Access to features in TEAMS or all of TEAMS for the user may be suspended.
    - The user will need to discuss the issues with a member of pastoral or leadership before reinstatement.
    - A pupil's parent/carer will be informed.

Using Microsoft Teams:

How to install the APP: Pupils Guide to Microsoft Teams - Installing Teams on your Device at Home-YouTube

Using Microsoft Teams: Pupils Guide to Microsoft Teams - Introducing your new Virtual Classroom - YouTube

Social Media - Expectations

- Pupils' use of social media platforms is the responsibility parents and carers, however, when it is used to have a detrimental impact on pupils or staff, it will not be tolerated.
- The expectations regarding safe and responsible use of social media applies to all members of Fairfield High School for Girls.
- The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.
- All members of the school are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- We will control pupil access to social media whilst using setting provided devices and systems on site.
- Concerns regarding the online conduct of any member of Fairfield High School for Girls community on social media, should be reported to the DSL (or Deputy DSL) and will be managed in accordance with our anti-bullying, allegations against staff, behaviour and child protection policies.

Pupils personal use of Social Media

- Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive education approach, via age appropriate sites and resources.

- Any concerns regarding pupils' use of social media will be dealt with in accordance with existing policies, including the Policy for Anti-bullying and the Policy for Outstanding Conduct and Behaviour.
    - Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.
- Pupils will be advised:
    - To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.
    - To only approve and invite known friends on social media sites and to deny access to others by making profiles private.
    - Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
    - To use safe passwords.
    - To use social media sites which are appropriate for their age and abilities.
    - How to block and report unwanted communications.
    - How to report concerns both within the setting and externally.

Use of Personal Devices and Mobile Phones - Expectations

All use of personal devices (including but not limited to; tablets, games consoles and 'smart' watches) and mobile phones will take place in accordance with the law and other appropriate policies, such as the Policy for Anti-bullying, the Policy for Outstanding Conduct and Behaviour and the Policy for Child Protection and Safeguarding.

Electronic devices of any kind that are brought onto site are the **responsibility of the user.**

- All pupils are advised to take steps to protect their mobile phones or devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school; any breaches will be dealt with as part of our Policy for Outstanding Conduct and Behaviour.

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.

- Pupils may bring mobile devices into school but are not permitted to use them at any time while on school premises. There can be exceptions to this rule authorised by the Headteacher or Deputy Headteacher.
- Fairfield High School for Girls expects pupils' personal devices and mobile phones to be switched off and out of sight at all times during the school day on the school site.
- If a pupil needs to contact their parent/carer they need to go to the Hub during break or lunchtime.
- If a pupil breaches the policy, the phone or device will be confiscated and will be held in a secure place.
    - Searches of mobile phone or personal devices will only be carried out in accordance with our policy. (www.gov.uk/government/publications/searching-screening-and-confiscation)
    - Pupils' mobile phones or devices may be searched by a member of the Senior Leadership Team, with the consent of the pupil or a parent/carer. Content may be deleted or requested to be deleted, if it contravenes our policies. (www.gov.uk/government/publications/searching-screening-and-confiscation)
    - If there is 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.

- 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 cancellation of the paper, disqualification from the subject or the disqualification from all subjects to be taken with the examination board.

Responding to Online Safety Incidents and Concerns

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our Acceptable Use Agreement and Code of Practice for Internet Access and Use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

- The DSL (or Deputy DSL) will be informed of any online safety incidents involving safeguarding or child protection concerns.
- The DSL (or Deputy DSL) will record these issues in line with our Policy for Child Protection and Safeguarding.
- The DSL (or Deputy DSL) will ensure that online safety concerns are escalated and reported to relevant agencies in line procedures.
- We will inform a parent/carer of online safety incidents or concerns involving their child, as and when required.

Procedures for Responding to Specific Online Incidents or Concerns

Online Sexual Violence and Sexual Harassment between Children

- Our school has accessed and understood "Sexual violence and sexual harassment between children in schools and colleges" (2021) guidance and part 5 of 'Keeping children safe in education' (2023).
- The school recognises that sexual violence and sexual harassment between children can take place online. Examples may include; non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation.
- The school will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our Life Skills and RSE curriculum.
- The school will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children.
- The school will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.
- If made aware of online sexual violence and sexual harassment, we will:
    - Immediately notify the DSL (or Deputy DSL) and act in accordance with our Policy for Child Protection and Safeguarding and Policy for Anti-bullying.

Youth Produced Sexual Imagery ("Sexting")

- The school recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or Deputy DSL).
- We will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people'.
- The school will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods. (including assemblies, Life Skills programme and working with the local Police liaison)

- If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:
  - Act in accordance with our child protection policies and the relevant Safeguarding Children Board's procedures.
  - Ensure the DSL (or Deputy DSL) responds in line with the 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.

Online Child Sexual Abuse and Exploitation (including child criminal exploitation)

- The school will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.
- The school recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or Deputy DSL).
- We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for pupils.
- We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.
- We will ensure that the 'Click CEOP' report button is visible and available to pupils and other members of our community. This is available on the website.
- If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:
  - Act in accordance with our Policy for Child Protection and Safeguarding and the relevant Safeguarding Children Board's procedures.

Online Hate, radicalisation and extremism

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at by the school and will be responded to in line with existing Policy for Anti-bullying and Policy for Outstanding Conduct and Behaviour.
- We will take all reasonable precautions to ensure that pupils are safe from terrorist and extremist material when accessing the internet on site. Internet use is monitored through the *Baracuda and *ESafe systems with daily reporting of risk categories to the safeguarding team.
- If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or Deputy DSL) will be informed immediately, and action will be taken in line with our child protection policy.

Links with other policies

This e-safety policy is linked to our:

- Policy for Child Protection and Safeguarding
- Policy for Outstanding Conduct and Behaviour
- Policy for Data Protection and Privacy Notices
- Policy for School Complaints
- Acceptable Use Agreements

National Links and Resources for Parents/Carers

- 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
- National Online Safety

APPENDIX 1: KS3 AND KS4 ACCEPTABLE USE AGREEMENT (PUPILS AND PARENT/CARER)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy **When I use the school's ICT systems (like computers) and get onto the internet in school I will:** • Always use the school's ICT systems and the internet responsibly and for educational purposes only • Only use them when a teacher is present, or with a teacher's permission • Keep my username and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Always ask permission from the owner before using any materials on the internet or credit the source. • Always respect the privacy of files of others • Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others • Always log off or shut down a computer when I'm finished working on it **I will not:** • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Log in to the school's network using someone else's details • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **If I bring a personal mobile phone or other personal electronic device into school:** • I will not use it while on school grounds including during lessons, tutor group time, clubs or other activities organised by the school. **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/Carer's Agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (Parent/Carer):	**Date:**