WHITFIELD ASPEN SCHOOL	Learning Together with Aspiration, Imagination, Determination	
Policy title: ONLINE SAFETY AND ICT ACCEPTABLE USE	Policy Status: AGREED	Policy Number: POL_043
Author(s): LA/John Dillon/Amanda Wood	Issue Date: 21st October 2026	Version: 4.0

Key Details

Designated Safeguarding Lead (s): Jason Cook, DSL/Headteacher

Named governor(s) with lead responsibility -

Safeguarding: Vicki Wood

IT Monitoring: Roger Knight

Core Regulatory Alignment: KCSIE,

Prevent Duty, UKCIS, UK GDPR

Primary Technical Infrastructure:

Fortinet (Fastvue), NCS, EIS

Date written/updated: October 2026

Date agreed and ratified by governing body: 21st October 2026

Date of next review: Summer 2027

This policy will be reviewed **at least** annually. It will also be revised following any changes to technology use, online safety concerns and/or updates to national and local guidance or procedures.

1. Policy Aims and Scope

- This policy has been written by Whitfield Aspen, involving staff, pupils and parents/carers, building on Kent County Councils Education Safeguarding Services policy template, with specialist advice and input as required. It takes into account the DfE statutory guidance 'Keeping Children Safe in Education', Early Years and Foundation Stage (**if applicable to the school**) 'Working Together to Safeguard Children' and our Kent Safeguarding Children Multi-agency Partnership procedures.
    - Education Safeguarding Service - KELSI
    - Home - Kent Safeguarding Children Multi-Agency Partnership (kscmp.org.uk)

- We recognise that online safety is an essential part of safeguarding and acknowledge our duty to ensure that all pupils and staff are protected from potential harmful and inappropriate online material and/or behaviour. This policy sets out our whole school approach to online safety which will empower, protect and educate our pupils and staff in their use of technology and establishes the mechanisms in place to identify, intervene in, and escalate any concerns where appropriate.

- Whitfield Aspen understands that breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:
    - **content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
    - **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
    - **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, for example, consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.
    - **commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

- Whitfield Aspen recognises that children are at risk of abuse online as well as face to face. In many cases abuse will take place concurrently via online channels and in daily life. Children can also abuse other children online.

- This policy applies to pupils, parents/carers and all staff, including the governing body, leadership team, 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).

- Whitfield Aspen identifies that the internet and technology, including computers, tablets, mobile phones, smart watches, games consoles and social media, is an important part of everyday life, and presents positive and exciting opportunities, as well as challenges and risks. This policy applies to all access to and use of technology, both on and off-site.

- Staff Whitfield Aspen recognise that children – **particularly those with profound, severe, and complex needs (PSCN)** – may not feel ready or know how to tell someone that they are being abused, exploited, or neglected online, and/or they may not recognise their experiences as being abusive or harmful. This should not prevent staff from having professional curiosity and speaking to a

DSL if they have any online safety concerns about a child.

- This policy links with several other policies, practices and action plans, including but not limited to:
    - Anti-bullying policy
    - Acceptable Use Policies (AUP)
    - AI policy *NEW* (POL_090)
    - Code of conduct/staff behaviour policy
    - Behaviour policy
    - Child protection policy
    - Confidentiality policy
    - Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE)
    - Data protection
    - Data Protection Complaints Process *NEW* (POL_089)
    - Data/information security
    - Cameras and image use policy (CCTV)

2. Responding to Emerging Risks

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

- We will:
    - carry out an annual review of our online safety approaches which will be supported by an annual risk assessment which considers and reflects the specific risks our pupils face.
    - regularly review the methods used to identify, assess and minimise online risks.
    - examine emerging technologies for educational benefit and undertake appropriate risk assessments before their use is permitted.
    - ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that internet access is appropriate.
    - recognise that due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our systems, and as such identify clear procedures to follow if breaches or concerns arise.

3. Policy monitoring and review

- Technology evolves and changes rapidly. Whitfield Aspen will review this policy at least annually. The policy will be revised following any national or local policy updates, any local concerns and/or any changes to our technical infrastructure.

- We will regularly monitor internet use taking place via our provided devices and systems and evaluate online safety mechanisms to ensure that this policy is consistently applied. Any issues identified will be incorporated into our action planning.

  To ensure they have oversight of online safety, the DSL/headteacher will be informed of online safety concerns, as appropriate.

- The named governor for safeguarding will report on online safety practice and incidents, including outcomes, on a regular basis to the wider governing body.

- All members of the community will be made aware of how our school will monitor policy compliance: Through staff updates and briefings; staff training (including subject leads and TAs). The policy will be shared with all staff and DBS regular staff who contribute to pupils learning.

4. Roles and Responsibilities

- The governing body have a strategic leadership responsibility for our school's online safeguarding arrangements; they will ensure that they comply with their duties under legislation and will ensure the policies, procedures and training in our school is effective and comply with the law at all times. Jason Cook, DSL/headteacher will ensure that the online safety policies and procedures, adopted by our governing bodies and proprietors, are understood, and followed by all staff.

  The Designated Safeguarding Lead (DSL) (Jason Cook, DSL/headteacher) has overall responsibility for the day-to-day oversight of safeguarding and child protection systems, including online safety and understanding the filtering and monitoring systems and processes in place. Whilst the activities of the DSL may be delegated to the deputies, the ultimate lead responsibility for online safety remains with the DSL and this responsibility will not be delegated.

- Whilst the DSL is recognised as holding overall lead responsibility for online safety, however Whitfield Aspen recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

4.1 Leadership and management

- The leadership team will:
  - Create a whole school culture that incorporates online safety throughout.
  - Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
  - Implement appropriate and up-to-date policies which address the acceptable use of technology, child-on-child abuse, use of social media and mobile technology.
    Work with the DSL and Fortinet (NSL, Cantium and local Network Manager) to ensure that suitable and appropriate filtering and monitoring systems are in place but hold overall responsibility for procuring our filtering and monitoring systems, documenting decisions on what is blocked or allowed and why, reviewing the effectiveness of our provision and overseeing any reports.
  - Support the DSL and any deputies by ensuring they have enough time and resources to carry out their responsibilities.
  - Ensure robust reporting channels are in place regarding online safety concerns.
  - Undertake appropriate risk assessments regarding the safe use of technology on site.
  - Audit and evaluate online safety practice to identify strengths and areas for improvement. Ensure that staff, pupils and parents/carers are proactively engaged in activities which promote online safety.
  - Support staff to ensure that online safety is embedded within a progressive whole school curriculum which enables all pupils to develop an appropriate understanding of online safety.

4.2 The Designated Safeguarding Lead (DSL):

- The leadership team will:
  - Act as a named point of contact on all online safeguarding issues.
  - Liaise with other members of staff, such as pastoral support staff, IT technicians, network managers and the SENCO on matters of online safety as appropriate.
    Ensure referrals are made to relevant external partner agencies, as appropriate.
  - Work alongside deputy DSLs to ensure online safety is recognised as part of our safeguarding responsibilities, and that a coordinated whole school approach is implemented.
  - Taking lead responsibility for overseeing and acting on any concerns identified by our filtering and monitoring systems (Fortinet (Fastvue)).
  - Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant and up-to-date knowledge required to keep pupils safe online, including the additional risks that pupils with Special Educational Needs and Disabilities (SEND) face online.
  - Ensure all members of staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and child protection training.
  - Keep up to date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
  - Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
  - Ensure that online safety is promoted to parents/carers and the wider community through a variety of channels and approaches.
  - Maintain records of online safety concerns as well as actions taken, as part of the schools safeguarding recording mechanisms (Iris Adapt – IRIS Adapt © 2008-22 Adaptsoft
  - Monitor online safety incidents to identify gaps and trends and use this data to update the education response and school policies and procedures.
  - Report online safety concerns, as appropriate, to the senior leadership team and Governing Body (via Iris Adapt – open door policy).
  - Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
  - Meet regularly (termly) with the governor with a lead responsibility for safeguarding.
  - Maintain a central point (Sharepoint) for reporting concerns over the use of age-inappropriate toys and/or talking about games/YouTube animations they are watching.

4.3 Members of staff

- It is the responsibility of all members of staff to:
  - Contribute to the development of our online safety policies.
  - Read and adhere to our online safety policy and acceptable use of technology policies.
  - Take responsibility for the security of IT systems and the electronic data they use or have access to.
  - Model good practice when using technology with pupils.

- Maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the pupils in their care.
- Identify online safety concerns and take appropriate action by following our safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including reporting to the DSL and signposting pupils and parents/carers to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.
- Maintain an open door policy.

4.4 IT Service Providers

- It is the responsibility of IT Staff, Cantium and Fortinet (Fastvue) managed by NCS who are managing our technical environment to:
  - Provide technical support and perspective to the DSL and leadership team in the development and implementation of our online safety policies and procedures, including appropriate filtering and monitoring systems.
  - Support the leadership team and DSL to procure systems, identify risk, carry out reviews and carry out checks to our filtering and monitoring systems.
    - Whilst responsibility for the procurement and implementation of appropriate filtering and monitoring is held by the leadership team and responsibility for acting on safeguarding concerns is led by the DSL; technical staff will ensure appropriate technical support and access to our filtering and monitoring systems is given to the DSL to enable them to take appropriate safeguarding action when required.
  - Implement appropriate security measures including (filtering and monitoring of designated harmful websites) as directed by the leadership team to ensure that the schools IT infrastructure is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.

4.5 Pupils

- It is the responsibility of pupils (at a level that is appropriate to their individual age and ability) to:
  - Engage in age/ability appropriate online safety education.
  - Contribute to the development of online safety policies.
  - Read and adhere to the acceptable use of technology and behaviour policies.
  - Respect the feelings and rights of others, on and offline.
  - Take an appropriate level of responsibility for keeping themselves and others safe online.
  - Seek help from a trusted adult, if they are concerned about anything, they or others experience online.

4.6 Parents/carers

- It is the responsibility of parents and carers to:

- Read our Acceptable Use of technology policies and encourage their child(ren) to adhere to them (see Home School Agreement).
- Support our online safety approaches by discussing online safety issues with their child(ren) and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media and abide by the home-school agreement and acceptable use of technology policies.
- Seek help and support from the school or other appropriate agencies if they or their child(ren) encounter online issues.
- Contribute to the development of our online safety policies.
- Use our systems, such as learning platforms and other IT resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by the new and emerging technologies that their child(ren) access and use at home.

4.7 Governing Body Oversight and Framework Compliance

- The governing body, supported by the named safeguarding and IT monitoring governors, maintains active oversight of online safety practises, filtering efficacy and filtering bypass logs.
- Online safety data, incident trends, and filtering reports are reviewed termly to evaluate the impact of our safeguarding measures and ensure alignment with statutory guidance and the OFSTED inspection framework (specifically regarding safeguarding culture, leadership oversight and personal development).

5. Education and Engagement Approaches

5.1 Education and engagement with Pupils

- Whitfield Aspen will establish and embed a whole school culture and will empower our pupils to acquire the knowledge needed to use the technology in a safe, considered and respectful way, and develop their resilience so they can manage and respond to online risks.

- We and will raise awareness and promote safe and responsible internet use amongst pupils by:
  - ensuring our curriculum and whole school approach is developed in line with the UK Council for Internet Safety (UKCIS) 'Education for a Connected World Framework' and DfE 'Teaching online safety in school' guidance.
  - ensuring online safety is addressed in Relationships Education, Relationships and Sex Education, Health Education, Citizenship and Computing programmes of study.
  - reinforcing online safety principles in other curriculum subjects and whenever technology or the internet is used on site.
  - Implementing appropriate peer education approaches.
  - creating a safe environment in which all pupils feel comfortable to say what they feel, without fear of getting into trouble and/or being judged for talking about something which happened to them online.
  - involving the DSL as part of planning for online safety lessons or activities, so they can advise on any known safeguarding cases, and ensure support is in place for any pupils who may be impacted by the content. The Designated teacher will plan online safety lesson and any concerns will be shared with DSL/SENCO before lesson commences.

- making informed decisions to ensure that any educational resources used are appropriate for our pupils.
- using external visitors, where appropriate, to complement and support our internal online safety education approaches. **'**Using External Visitors to Support Online Safety Education: Guidance for Educational Schools**'.**
- providing online safety education as part of the transition programme across the key stages or when moving between establishments.
- rewarding positive use of technology.

- Whitfield Aspen will support pupils to understand and follow our Acceptable Use policies in a way which suits their age and ability**.**
  - sharing our acceptable use policies with them in accessible and appropriate ways.
  - 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.
  - seeking pupils voice when writing and developing online safety policies and practices, including curriculum development and implementation.

- Whitfield Aspen will ensure pupils develop the underpinning knowledge and behaviours needed to navigate the online world safely, in a way which suits their age and ability by:
  - ensuring age and/or ability appropriate education regarding safe and responsible use precedes internet access.
  - enabling them to understand what acceptable and unacceptable online behaviour looks like.
  - teaching pupils to evaluate what they see online and recognise techniques used for persuasion, so they can make effective judgements about if what they see is true, valid or acceptable.
  - educating them in the effective use of the internet to research, including the skills of knowledge location, retrieval and evaluation.
  - preparing them to identify possible online risks and make informed decisions about how to act and respond.
  - ensuring they know how and when to seek support if they are concerned or upset by something they see or experience online.

5.2 Vulnerable Pupils and those who are potentially at greater risk of harm

- Whitfield Aspen recognises that any pupils can be vulnerable online, and vulnerability can fluctuate depending on age, developmental stage and personal circumstances. However, there are some pupils, for example, looked after children, child who are care leavers, children who are adopted, children who are, or who are perceived to be, lesbian, gay, bi, or trans (LGBT), and those with special educational needs or disabilities (SEND), who may be more susceptible or may have less support in staying safe online.

- Whitfield Aspen School will ensure that highly differentiated, accessible, and appropriate online safety education, communication tools and support are provided to all children who require additional or targeted assistance, paying specific regard to our high proportion of children with Special Educational Needs and Disabilities (SEND) and those within our Profound, Severe and Complex Needs (PSCN) provision.

- Staff at Whitfield Aspen School will actively seek input from specialist staff, including the DSL, SENCO, SRP Leads and Designated Teacher, to ensure that the policy, assistive technologies and curriculum remain fully inclusive and adapted to our community's complex needs.

5.3 Training and engagement with staff

- We will:
    - provide and discuss the online safety policy and procedures, including our acceptable use policy, with all members of staff, including governors as part of induction.
    - provide up-to-date and appropriate training for all staff, including governors, which is integrated, aligned and considered as part of our overarching safeguarding approach.
    - ensure our training for governors equips them with the knowledge to provide strategic challenge to test and assure themselves that our online safety policies and procedures in place in are effective and support the delivery of a robust whole school approach.
    - ensure that online safety training provided to all staff is regularly updated. We will provide training annually (until reviewed) using the training day allocated in the school year by the LA.
    - ensure our training covers the potential risks posed to pupils (content, contact and conduct) as well as our professional practice expectations.
    - build on existing expertise, by providing opportunities for staff to contribute to and shape our online safety approaches.
    - ensure staff are aware that our IT systems are monitored, and that activity can be traced to individual users. Staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
    - ensure staff are aware that their online conduct, including personal use of social media, can have an impact on their professional role and reputation.
    - highlight useful educational resources and tools which staff could use with pupils.
    - ensure all members of staff are aware of the procedures to follow regarding online safety concerns involving pupils, colleagues or other members of the community.

5.4 Awareness and engagement with parents and carers

- Whitfield Aspen recognises that parents and carers have an essential role to play in enabling our pupils to become safe and responsible users of the internet and associated technologies.

- We will ensure parents and carers understand and are aware of:
    - the systems used at school to filter and monitor their child's online use by including this detail in Home School Agreements (and signing of age appropriate Acceptable Use policy (AUP) agreement).
    - what their children are being asked to do online, including the sites they will asked to access and be clear who from the school (if anyone) their child is going to be interacting with online by providing information in our home-school agreement/AUP'.

- We will build a partnership approach and reinforce the important of online safety through regular contact and communication 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, transition events, fetes and sports days.
- drawing their attention to our online safety policy and expectations in our newsletters and other external communication (such as letters and social media channels) as well as in our on our website.
- requesting parents and carers read online safety information as part of joining our community, for example, within our home school agreement.
- requiring them to read our acceptable use of technology policies and discuss the implications with their children.

5.5 Specialised Online Safety and Accessibility for PSCN and SEND Learners

- Whitfield Aspen School recognises that children with Special Education Needs and Disabilities (SEND), and particularly those within our Profound, Severe and Complex Needs (PSCN) Specially Resourced Provision (SRP), may experience distinct vulnerabilities, differing cognitive capacities to assess online risk, and heightened exposure to grooming or online manipulation.
- We commit to providing tailored, multi-sensory, and accessible online safety messages using visual supports, social stories and augmented communication tools where appropriate.
- Staff will ensure that assistive technologies used by children are risk-assessed, secure and monitored to protect privacy while enabling full curriculum access.

6. Safer Use of Technology

6.1 Classroom use

- Whitfield Aspen uses a wide range of technology. This includes access to:
  - Computers, laptops, tablets and other digital devices
  - Internet, which may include search engines and educational websites
  - Learning platforms, remote learning platform/tools and intranet
  - Staff and Class Email
  - Digital cameras, webcams and video cameras.

- All school owned devices will be used in accordance with our acceptable use of computing policies 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. A Google safe search Fortinet (Fastvue) filtering and monitoring will take place.

- The school will use appropriate search tools as identified following an informed risk assessment.

- Use of video sharing platforms will be in accordance with our acceptable use of technology policies, following an informed risk assessment and with appropriate safety and security measures in place.

- 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 internet access and technology use will be appropriate to pupils age and ability.

Early Years Foundation Stage, Key Stage 1 and Key Stage 2

- Access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the pupils age and ability.

- **Key Stage 2**
  - Pupils will be directed to use age-appropriate search engines, online tools and apps.

6.2 Managing internet access

- All users will read and agree and/or acknowledge our acceptable use policy, appropriate to their age, understanding and role, before being given access to our computer system, IT resources or the internet. See Appendices 3, 4 or 5.

- We will maintain a record of staff who are granted access to our devices and systems. Guest Wi-Fi access is permitted to visitors run by Meraki (intranet).
- Astrosafe app (Webbrowser) has now taken the place of the browsers Google/Safari on the childrens ipads and tablets.

6.3 Managing personal data online

- Personal data will be recorded, processed, transferred and made available online in strict accordance with UK General Data Protection Regulations (UK GDPR) and current Data Protection of Data (Use and Access) Act 2025 (DUAA) legislation. See GDPR policy - Policies | Whitfield Aspen School or Information Commissioners Office (ICO) - Information Commissioner's Office (ICO).
- To ensure absolute compliance, independent technical oversight, and robust system auditing, Whitfield Aspen School partners directly with Data Protection Solutions. This external data governance specialist works alongside the Senior Leadership Team (SLT) and the designated School Data Protection Officer to maintain the absolute security of the school's information perimeter.
- All personal data systems are managed under the following regulatory and third-party parameters:

- **Regulatory Alignment**: Data pathways are continuously cross-referenced against the statutory guidelines provided by the Information Commissioners Office (ICO).
- **Third-Party Processing Standards**: **Data Protection Solutions** serves as a primary processor and auditing body, ensuring that any hosted or cloud-based storage system complies with strict data retention schedules, automated deletion protocols, and minimised access paths.
- **Complaint Pipeline Integration**: Any data-related breaches, parental tracking concerns, or information security exceptions identified by our systems or flagged by Data Protection

Solutions will be managed under the specific Data Protection Complaints Policy (POL_089), distinct from general school grievance procedures.

6.4 Information security and access management

- We take appropriate steps to ensure necessary security protection procedures are in place, in order to safeguard our systems, staff and pupils.

- Further information about technical environment safety and security can be found in….
    - Virus protection being updated regularly.
    - Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
    - Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
    - Not downloading unapproved software to work devices or opening unfamiliar email attachments.
    - Preventing, as far as possible, access to websites or tools which could compromise our systems, including anonymous browsing and other filtering bypass tools.
    - Checking files held on our network, as required and when deemed necessary by leadership staff.
    - The appropriate use of user logins and passwords to access our network and user logins and passwords will be enforced for all users.
    - All users are expected to log off or lock their screens/devices if systems are unattended.

- Cantium will review the effectiveness of our security approaches and procedures periodically in order to keep up with evolving cyber-crime technologies by issuing warning emails and notices.

6.4.1 Password policy

To prevent unauthorised access, the school enforces a rigorous credential standard for all staff, visitors and pupils:-

- **Unique Accounts** : Every single staff member and pupil is allocated an individual, unique username and private password to track system accountability. Logging in as another user at any time is completely forbidden.
- **Password Complexity** : Users are required to generate “strong” passwords, which are defined as having **8 or more characters** and consisting of a mix of numbers, letters, and symbols.
- **Maintenance & Security** : Passwords must be changes **frequently**. Users are explicitly banned from sharing passwords or login credentials with peers, or leaving login details exposed where others can easily discover them.
- **Administrative Security** : The primary administrator account for the main school website must be independently secured using a unique, complex strong password.
- Lock access to devices/systems when not in use.

6.5 Managing the safety of our website

- We will ensure that information posted on our website meets the requirements as identified by the DfE.
- We will ensure that our school website complies with guidelines for publications, including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright.
- Staff or pupils' personal information will not be published on our website; the contact details on the website will be our school address, email and telephone number.
- The administrator account for our website will be secured with an appropriately strong password.
- We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

6.6 Publishing images and videos online

- We will ensure that all images and videos shared online are used in accordance with the associated policies, including (but not limited to) the cameras and image use, data security, acceptable use policies, codes of conduct/behaviour, social media and use of personal devices and mobile phones policies, in line with parental consent.

6.7 Managing email

- Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, acceptable use of technology policies and the code of conduct/behaviour policy.
- The forwarding of any chain messages/emails is not permitted.
- Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email or via a shared link.
- School email addresses and other official contact details will not be used to set up personal social media accounts.
- Members of the community will immediately report offensive communication to the DSL Team.
- Excessive social email use can interfere with teaching and learning and will be restricted; access to external personal email accounts may be blocked on site.

6.7.1 Staff email

- All members of staff:

- are provided with an email address to use for all official communication; the use of personal email addresses by staff for any official business is not permitted.
- are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, pupils and parents.

6.8 Educational use of videoconferencing and/or webcams

- Whitfield Aspen recognise that videoconferencing and use of webcams can be a challenging activity but brings a wide range of learning benefits.
  - All videoconferencing and webcam equipment will be switched off when not in use and will not be set to auto-answer.
  - Videoconferencing equipment connected to the educational broadband network will use the national E.164 numbering system and display their H.323 ID name; external IP addresses will not be made available to other sites.
  - Videoconferencing contact details will not be posted publicly.
  - Videoconferencing equipment will not be taken off the premises without prior permission from the DSL/DSL/headteacher. See SOP.
  - Staff will ensure that external videoconferencing opportunities **and/or** tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure. We will recommend using Teams where possible.
  - Videoconferencing equipment and webcams will be kept securely and, if necessary, locked away or disabled when not in use.

6.8.1 Users

- Parents/carers consent will be obtained prior to pupils taking part in videoconferencing activities**.**

- Videoconferencing will take place via official and approved communication channels following a robust risk assessment and will be supervised appropriately, according to the pupils age and ability. Pupils are not permitted to do the above unless an adult is present and it has been requested that the child attends.

- The unique log on and password details for the videoconferencing services will only be issued to members of staff and will be kept securely, to prevent unauthorised access.

6.8.2 Content

- When recording a videoconference lesson, it should be made clear to all parties at the start of the conference and written permission will be obtained from all participants, e.g. parents; the reason for the recording must be given and recorded material will be stored securely.

- If third party materials are included, we will check that recording is permitted to avoid infringing the third-party intellectual property rights.

- We will establish dialogue with other conference participants before taking part in a videoconference; if it is a non-educational site, staff will check that the material they are delivering is appropriate for the Pupils.

6.9 Management of applications (apps) used to record progress

- We do currently use an app (Evidence for Learning) to track pupil progress and share appropriate information with parents and carers.

- The DSL/headteacher will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that use takes place in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.

- To safeguard student data:
    - only school issued devices will be used for apps that record and store Pupils' personal details, attainment or photographs.
    - personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store Pupils personal details, attainment or images.
    - devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
    - all users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
    - parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

6.10 Management of remote learning

Where children are asked to learn online at home in response to a full or partial closure:

- Whitfield Aspen will ensure any remote sharing of information, communication and use of online learning tools and systems will be in line with privacy and data protection requirements.

- All communication with pupils and parents/carers will take place using school provided or approved communication channels; for example, school provided email accounts and phone numbers or agreed systems: TT Rockstars, Reading Theory, Renaissance, Busy Things, Word Shark, Arithmagicians.
    - Any pre-existing relationships or situations which mean this cannot be complied with will be discussed with the DSL.

- Staff and pupils will engage with remote teaching and learning in line with existing behaviour principles as set out in our behaviour policy/code of conduct and Acceptable Use Policies.

- Staff and pupils will be encouraged to report issues experienced at home and concerns will be responded to in line with our child protection and other relevant policies.

- When delivering remote learning, staff will follow our Remote Learning Acceptable Use Policy (AUP).

- Parents/carers will be made aware of what their children are being asked to do online, including the sites they will be asked to access. Whitfield Aspen will continue to be clear who from the school their child is going to be interacting with online.

- Parents/carers will be encouraged to ensure children are appropriately supervised online and that appropriate parent controls are implemented at home.

6. Appropriate Filtering and Monitoring on School Devices and Networks

- Whitfield Aspen will do all we reasonably can to limit children's exposure to online harms through school provided devices and networks and in line with the requirements of the Prevent Duty, KCSIE and UK Safer Internet Centre (link - Homepage - UK Safer Internet Centre) we will ensure that appropriate filtering and monitoring systems are in place.

- When implementing appropriate filtering and monitoring, Whitfield Aspen will ensure that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.

- Whilst filtering and monitoring is an important part of our online safety responsibilities, it is only one part of our approach to online safety and we recognise that we cannot rely on filtering and monitoring alone to safeguard our pupils; effective safeguarding practice, robust policies, appropriate classroom/behaviour management and regular education/training about safe and responsible use is essential and expected.

  Pupils will use appropriate search tools, apps and online resources as identified by staff, following an informed risk assessment.

- Internet use will be supervised by staff as appropriate to pupils age, ability and potential risk of harm.

7.1 Responsibilities for filtering and monitoring

- Our governing body has overall strategic responsibility for our filtering and monitoring approaches, including ensuring that our filtering and monitoring systems are regularly reviewed, and that the leadership team and relevant staff have an awareness and understanding of the appropriate filtering and monitoring provisions in place, manage them effectively and know how to escalate concerns when identified.

- Members of the senior leadership team and the IT governor(s), are responsible for ensuring that our school has met the DfE Filtering and monitoring standards for schools and colleges.

- Our senior leadership team are responsible for, along with Cantium:
  - procuring our filtering and monitoring systems.
  - documenting decisions on what is blocked or allowed and why.
  - reviewing the effectiveness of our provision.
  - overseeing reports.
  - ensuring that all staff understand their role, are appropriately trained, follow policies, processes and procedures and act on reports and concerns (Iris).

- ensuring the DSL and Fortinet (Fastvue) have sufficient time and support to manage their filtering and monitoring responsibilities.

- The DSL has lead responsibility for overseeing and acting on:
  - any filtering and monitoring reports.
  - any child protection or safeguarding concerns identified.
  - checks to filtering and monitoring system.

- The IT service providers have technical responsibility for:
  - maintaining filtering and monitoring systems.
  - providing filtering and monitoring reports (these are emailed from Fortinet (Fastvue)).
  - completing technical actions identified following any concerns or checks to systems.
  - working with the senior leadership team and DSL to procure systems, identify risks, carry out reviews and carry out checks.

- All members of staff are provided with an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring as part of our induction process, and in our child protection staff training.

- All staff, pupils and parents/carers have a responsibility to follow this policy to report and record any filtering or monitoring concerns.

7.2 Decision making and reviewing our filtering and monitoring provision

- When procuring and/or making decisions about our filtering and monitoring provision, our senior leadership team works closely with the DSL and the IT service providers. Decisions have been recorded and informed by an approach which ensures our systems meet our schools' specific needs and circumstances, including but not limited to our student risk profile and specific technology use.

- Any changes to the filtering and monitoring approaches will be assessed by staff with safeguarding, educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.

- Our school undertakes an at least annual review of our filtering and monitoring systems to ensure we understand the changing needs and potential risks posed to our community.

- In addition, our school undertakes regular checks on our filtering and monitoring systems, which are logged and recorded, to ensure our approaches are effective and can provide assurance to the governing body that we are meeting our safeguarding obligations.

7.3 Appropriate filtering

DfE's filtering and monitoring standards – see Appendix 2.

Whitfield Aspen's education broadband connectivity is provided through our internet service provider (BT/ NCS) and Whitfield Aspen uses Fortinet (Fastvue) to filter and monitor.

- Fortinet (Fastvue) is a member of Internet Watch Foundation (IWF). Leaders should check to ensure this is the case.

- Fortinet (Fastvue) has signed up to Counter-Terrorism Internet Referral Unit list (CTIRU) Leaders should check to ensure this is the case.

  Fortinet (Fastvue) is blocking access to illegal content including child sexual abuse material (CSAM).

  Fortinet (Fastvue) blocks access to sites which could promote or include harmful and/or inappropriate behaviour or material. This includes content which promotes discrimination or extremism, drugs/substance misuse, malware/hacking, gambling, piracy and copyright theft, pro-self-harm, eating disorder and/or suicide content, pornographic content and violent material.

- We filter internet use on all school owned, or provided, internet enabled devices and networks.

- Our filtering system is operational, up to date and is applied to all users, including guest accounts, all school owned devices and networks, and all devices using the school broadband connection.

- We work with our ISP and our staff to ensure that our filtering policy is continually reviewed to reflect our needs and requirements.

- If there is failure in the software or abuse of the system, for example if pupils or staff accidentally or deliberately access, witness or suspect unsuitable material has been accessed, they are required to alert a DSL by supplying the following information:- IP address, Device ID (MAC) and device name.

- Filtering breaches will be reported to the DSL and technical staff and will be recorded and escalated as appropriate and in line with relevant policies, including our child protection, acceptable use, allegations against staff and behaviour policies.

  Parents/carers will be informed of filtering breaches involving their child.

- Any access to material believed to indicate a risk of significant harm, or that could be illegal, will be reported as soon as it is identified to the appropriate agencies, including but not limited to the Internet Watch Foundation (where there are concerns about child sexual abuse material), the police (either via 101 or 999 if an emergency or NCA-CEOP) or Children's Social Care.

- If staff are teaching topics which could create unusual activity on the filtering logs, or if staff perceive there to be unreasonable restrictions affecting teaching, learning or administration, they will report this to the DSL and/or leadership team.

7.4 Appropriate monitoring

- We will appropriately monitor internet use on all school provided devices and networks using the topic in 7.3 Appropriate filtering (filtering breaches).

- All users will be informed that use of our devices and networks can/will be monitored and that all monitoring is in line with data protection, human rights and privacy legislation as well as our Acceptable Use Policy (AUP). See Appendices 3, 4 or 5.

- If a concern is identified via our monitoring approaches:
  - Where the concern relates to pupils, it will be reported to the DSL/headteacher and will be recorded and responded to in line with relevant policies, such as child protection, acceptable use, and behaviour policies.
- Where the concern relates to staff, it will be reported to the DSL/headteacher (or chair of governors if the concern relates to the DSL/headteacher), in line with our staff behaviour/allegations (or Whistleblowing) policy.
- Where our monitoring approaches detect any immediate risk of harm or illegal activity, this will be reported as soon as possible to the appropriate agencies; including but not limited to, the emergency services via 999, the Police via 101 or NCA-CEOP , the LADO or Children's Social Care.

7. Social Media

8.1 Expectations

- Whitfield Aspen believes everyone should be treated with kindness, respect and dignity. Even though online spaces may differ in many ways, the same standards of behaviour are expected online as offline, and all members of our community are expected to engage in social media in a positive and responsible manner.

- All members of our community are advised not to post or share content that may be considered threatening, hurtful or defamatory to others on any social media service.

- We will restrict learner and staff access to social media via our filtering and monitoring systems which are applied to all school provided devices and systems; further information on how this is achieved in addressed in our child protection policy.

- Inappropriate or excessive use of social media during school hours or whilst using school devices e.g. mobile phones) may result in removal of internet access and/or disciplinary action.

- The use of social media or apps, for example as a formal remote learning platform or education tool will be robustly risk assessed by the DSL and/or DSL/headteacher prior to use with learners. Any use will take place in accordance with our existing policies, for example, child protection, staff/learner behaviour acceptable use policies, remote learning Acceptable Use Policy.

- Concerns regarding the online conduct of any member of the Whitfield Aspen community on social media will be taken seriously. Concerns will be managed in accordance with the appropriate policies, including anti-bullying, allegations against staff, behaviour, home school-agreements, staff behaviour/code of conduct, Acceptable Use Policies, and child protection.

8.2 Staff use of social media

- The use of social media during school hours for personal use is not appropriate for staff.

- Safe and professional online behaviour is outlined for all members of staff, including volunteers, as part of our code of conduct/behaviour policy and/or acceptable use of computing policy.

- The safe and responsible use of social media sites will be discussed with all members of staff as part of staff induction. Advice will be provided and updated via staff training and additional guidance and resources will be shared with staff as required on a regular basis.

- Any complaint about staff misuse of social media or policy breaches will be taken seriously in line with our child protection and allegations against staff policy.

8.2.1 Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the school. Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

- All members of staff are advised to safeguard themselves and their privacy when using social media. This may include, but is not limited to:
    - Setting appropriate privacy levels on their personal accounts/sites.
    - Being aware of the implications of using location sharing services.
    - Opting out of public listings on social networking sites.
    - Logging out of accounts after use.
    - Using strong passwords.
    - Ensuring staff do not represent their personal views as being that of the school.
- Members of staff are encouraged not to identify themselves as employees of Whitfield Aspen on their personal social networking accounts; this is to prevent information being linked with the setting and to safeguard the privacy of staff members.

- All staff are expected to ensure that their social media use is compatible with their professional role and is in accordance our policies and the wider professional reputation and legal framework. All members of staff are encouraged to carefully consider the information, including text and images, they share and post on social media.

- Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members or colleagues, will not be shared or discussed on social media sites.

- Members of staff will notify the leadership team immediately if they consider that any content shared on social media sites conflicts with their role.

8.2.2 Communicating with Pupils and their families

- Staff will not use any personal social media accounts to contact pupils or their family members.
- All members of staff are advised not to communicate with or add any current or past pupils or their family members, as 'friends' on any personal social media accounts.
- Any communication from pupils and parents/carers received on personal social media accounts will be reported to the DSL (or deputy) or the DSL/headteacher.
- Any pre-existing relationships or situations, which mean staff cannot comply with this requirement, will be discussed with the DSL and the DSL/headteacher. Decisions made and advice provided in these situations will be formally recorded to safeguard pupils, members of staff and the setting.
- If ongoing contact with pupils is required once they have left the setting, members of staff will be expected to use existing alumni networks, or use official setting provided communication tools.

8.3 Official use of social media

- Whitfield Aspen has official social media channels i.e. Facebook https://www.facebook.com/whitfieldaspenprimary
- The official use of social media sites by Whitfield Aspen only takes place with clear educational or community engagement objectives and with specific intended outcomes and once the use has been formally risk assessed and approved by the DSL/headteacher prior to use.
- Official social media sites are suitably protected and, where possible, run **and** linked **from** our school website.
    - Official social media channels have been set up as distinct and dedicated accounts for official educational or engagement purposes only.
    - Staff use setting provided email addresses to register for and manage official social media channels.
    - Leadership staff have access to account information and login details for our social media channels, in case of emergency, such as staff absence.
- Official social media use will be conducted in line with existing policies, including but not limited to anti-bullying, image/camera use, data protection, confidentiality and child protection.
- All communication on official social media platforms by staff on behalf of the setting will be clear, transparent and open to scrutiny. Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by at least one other colleague.
- Parents/carers and pupils will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
- Parents and carers will be informed of any official social media use with pupils; any official social media activity involving pupils will be moderated if possible and written parental consent will be obtained as

required.

- We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

- Members of staff who follow and/or like our official social media channels will be advised to use dedicated professionals accounts where possible, to avoid blurring professional boundaries.

- If members of staff are managing and/or participating in online social media activity as part of their capacity as an employee of the setting, they will:
    - Read and understand our Acceptable Use Policy.
    - Where they are running official accounts, sign our social media Acceptable Use Policy.
    - Be aware they are an ambassador for the school.
    - Be professional, responsible, credible, fair and honest, and consider how the information being published could be perceived or shared.
    - Always act within the legal frameworks they would adhere to within the workplace, including libel, defamation, confidentiality, copyright, data protection and equalities laws.
    - Follow our image use policy at all times, for example ensuring that appropriate consent has been given before sharing images.
    - Not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so.
    - Not engage with any private or direct messaging with current or past pupils or their family members.
    - Inform their line manager, the DSL (or deputy) and/or the DSL/headteacher of any concerns, such as criticism, inappropriate content or contact from pupils.

8.4 Pupils use of social media

- The use of social media during school hours for personal use is not permitted for pupils.

- Many online behaviour incidents amongst children and young people occur on social media outside the school day and off the school premises. Parents/carers are responsible for this behaviour; however, some online incidents may affect our culture and/or pose a risk to children and young people's health and well-being. Where online behaviour online poses a threat or causes harm to another Pupils, could have repercussions for the orderly running of the school when the pupils is identifiable as a member of the school, or if the behaviour could adversely affect the reputation of the school, action will be taken in line with our behaviour and child protection/online safety policies.

- Whitfield Aspen will empower our pupils to acquire the knowledge needed to use social media in a safe, considered and respectful way, and develop their resilience so they can manage and respond to online risks. Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive safeguarding education approach using age-appropriate sites and resources. Further information is contained within our child protection and relevant specific curriculum policies.

- We are aware that many popular social media sites are not permitted for use by children under the age of 13, or in some cases higher. As such, we will not create accounts for pupils under the required age as outlined in the services terms and conditions.

- Pupils will be advised:
  - to consider the benefits and risks of sharing personal details or information 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, for example by making profiles private.
  - not to meet any online friends without a parent/carer or other appropriate adults' permission, and to only do so when a trusted adult is present.
  - to use safe passwords and not share with any other peers, inside or outside school.
  - to use social media sites which are appropriate for their age and abilities.
  - how to block and report unwanted communications.
  - how to report concerns on social media, both within the setting and externally.

- Any concerns regarding pupils use of social media will be dealt with in accordance with appropriate existing policies, including anti-bullying, child protection and behaviour.

- The DSL (or deputy) will respond to social media concerns involving safeguarding or child protection risks in line with our child protection policy.

- Sanctions and/or pastoral/welfare support will be implemented and offered to pupils as appropriate, in line with our child protection and behaviour policy. Civil or legal action may be taken if necessary.

- Concerns regarding pupils use of social media will be shared with parents/carers as appropriate, particularly when concerning underage use of social media services and games.

8.5 Child-Centred AI Online

Child-Centred Artificial Intelligence (AI)

We are committed to ensuring that any use of artificial intelligence (AI) within our online settings respects and protects the rights, safety, and well-being of children.

Regulatory Compliance and Oversight

We ensure that AI systems used within our online setting comply with applicable laws, regulations, and recognised standards relating to children, online safety, and data protection. Appropriate governance, monitoring, and review mechanisms are maintained to oversee AI-enabled systems that may affect children.

These are how we use AI in school:

1. Ensure **regulatory** frameworks, oversight and compliance for child-centred AI
2. Ensure **safety** for children
3. Protect children's **data and privacy**
4. Ensure **non-discrimination and fairness** for children
5. Provide **transparency, explainability and accountability** for children

6. Respect human and child rights through **responsible AI practice**
7. Support children's **best interests, development and well-being**
8. Ensure **inclusion** of and for children
9. Prepare and **skill** children for present and future developments in AI use
10. Create an **enabling environment** for child-centred AI

8.6 Adult Guidance for AI Use in Schools

Purpose

This guidance supports **adults working in Whitfield Aspen School** to use artificial intelligence (AI) **safely, ethically, and effectively**, while protecting **children**, staff, and school integrity.

8.6.1. Core Principles for Adults Using AI

Adults should use AI in ways that:

- **Support, not replace, professional judgement**
- **Protect pupil safety, privacy, and wellbeing**
- **Comply with safeguarding, GDPR, and data-protection law**
- **Promote fairness, inclusion, and transparency**
- **Model responsible AI use to pupils**

AI must always remain **a tool**, not a decision-maker. [gov.uk], [unesco.org]

8.6.2. Appropriate Uses of AI by Adults

Adults **may use AI** for:

- Lesson planning and resource drafting
- Differentiation ideas and scaffolding support
- Summarising policies or guidance
- Drafting letters or communications (with review)
- Creating low-stakes quizzes or discussion prompts
- Supporting workload reduction (e.g. planning templates)

All outputs **must be reviewed, checked for accuracy, and adapted** before use with pupils. [gov.uk], [roadmap-fo...ign.gov.uk]

8.6.3. Inappropriate or Prohibited Uses

Adults **must not**:

- Input **personal data** about pupils or staff into public AI tools
- Use AI to make **safeguarding, SEN, behavioural, or attainment decisions**

- Use AI to **grade high-stakes assessments without human review**
- Present AI-generated work as professional judgement
- Circumvent school policies using AI tools

DfE guidance is clear that AI outputs can be **inaccurate, biased, or fabricated**, and therefore must never be relied upon without verification. [gov.uk]

8.6.4. Data Protection and Safeguarding

Adults must:

- Treat AI tools as **third-party processors**
- Never upload:
    - Names of pupils or staff
    - Case details
    - Medical, safeguarding, or SEN information
- Use **school-approved platforms only**
- Report concerns immediately through safeguarding channels

This aligns with **UK GDPR**, DfE expectations, and safeguarding duties. [gov.uk], [roadmap-fo...ign.gov.uk]

A new policy and process for submission of Data Protection Complaints (POL_089) is available separate to the Complaints policy (October 2026).

8.6.5. Transparency and Professional Integrity

Adults should:

- Be **open** about using AI (where relevant)
- Explain to pupils **how AI assisted**, not replaced, the work
- Model critical thinking and ethical technology use
- Challenge inaccurate or biased AI outputs

UNESCO highlights that adults play a key role in teaching pupils to **question and evaluate AI outputs** rather than trust them blindly. [unesco.org]

8.6.6. Supporting Pupils' AI Use

Adults should:

- Teach pupils how AI works at a **developmentally appropriate level**
- Reinforce school rules on academic integrity
- Support ethical use rather than blanket bans
- Encourage pupils to:
    - Cite AI assistance where allowed
    - Think critically about accuracy and bias

DfE and UNESCO both emphasise **AI literacy** as a staff responsibility, not just a pupil skill. [gov.uk], [unesco.org]

A new policy on the use of A.I (POL_090). for all staff and anyone on school property, is available (October 2026).

8.6.7. Training and Ongoing Responsibilities

Adults are expected to:

- Complete relevant **AI training or briefings**
- Stay aware of emerging risks (deepfakes, misinformation)
- Follow school policy updates
- Raise concerns where AI use feels unsafe or inappropriate

Guidance should be treated as a **living document**, reviewed regularly as tools and risks evolve.

All members of staff will be provided with, and are required to read, part one of the current version of 'Keeping Children Safe in Education'.

8. Mobile and Smart Technology

- Our mobile and smart technology policy applies to all access to and use of all mobile and smart technology on site; this includes but is not limited to mobile/smart phones and personal devices such as tablets, e-readers, games consoles and wearable technology, such as smart watches and fitness trackers, which facilitate communication or have the capability to record sound and/or images.

9.1 Safe use of mobile and smart technology expectations

- Our school recognises that use of mobile and smart technologies is part of everyday life for many pupils, staff and parents/carers.

- Electronic devices of any kind that are brought onto site are the responsibility of the user. All members of our community are advised to:
    - take steps to protect their personal mobile phones or other smart devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
    - use passwords/PIN numbers to ensure that unauthorised access, calls or actions cannot be made on personal phones or devices.

  Mobile devices and other forms of smart technology are not permitted to be used in specific areas on site; this includes changing rooms, toilets and swimming pools.

- The sending of abusive or inappropriate messages or content, including via personal mobile devices and smart technology is forbidden by any member of the community; any breaches will be dealt with in line with our anti-bullying, behaviour and child protection policies.

- All members of our community are advised to ensure that their personal mobile and smart technology devices do not contain any content which may be offensive, derogatory or illegal, or which would otherwise contravene our behaviour or child protection policies.

9.2 School provided mobile phones and devices

- Some member of staff will be issued with a work phone number in addition to their work email address, where contact with pupils or parents/carers is required for every working day.
- Staff providing formal remote/online learning will do so using school provided equipment in accordance with our Acceptable Use Policy.
- School provided mobile phones will be suitably protected via a passcode/password/PIN and must only be accessed or used by members of staff.
- School provided mobile phones will always be used in accordance with our staff code of conduct/behaviour policy, acceptable use of computing policy and other relevant policies.
- Where staff and/or pupils are using school provided mobile phones and devices, they will be informed prior to use via our Acceptable Use Policy (AUP) that activity may be monitored for safeguarding reasons and to ensure policy compliance.
- Staff using their own personal mobile phone need to hide their number with the 141 prefix or, preferably, use a school phone.
- Class teachers will send emails from the class email account, to parents advising them about the use of mobile phones by **children** for the purposes of walking to and from school, **independently**. See Appendix 6 for the email wording.

9.3 Staff use of mobile and smart technology

- Members of staff will ensure that use of any mobile and smart technology, including personal phones, wearable technology and other mobile/smart devices, will take place in accordance with the law, as well as relevant school policy and procedures, such as confidentiality, child protection, data security, staff behaviour/code of conduct and Acceptable Use Policies. Amend as appropriate.

- Staff will be advised to:
    - Keep personal mobile and smart technology devices in a safe and secure place (list details, for example, locked in a locker/drawer) during lesson time.
    - Keep personal mobile phones and devices switched off or set to ‘silent’ or ‘do not disturb’ modes during lesson times.
    - Ensure that Bluetooth or other forms of communication, such as ‘airdrop’, are hidden or disabled during lesson times.
    - Not use personal mobile or smart technology devices during teaching periods, unless written permission has been given by the DSL/headteacher, such as in emergency circumstances.
    - Ensure that any content bought onto site via personal mobile and smart technology devices is compatible with their professional role and our behaviour expectations.
- Members of staff are not permitted to use their own mobile and smart technology devices for contacting Pupils or parents and carers.

  - Any pre-existing relationships or circumstance, which could compromise staff's ability to comply with this, will be discussed with the DSL and/or DSL/headteacher.
  - Staff using their own personal mobile phone need to hide their number with the 141 prefix or, preferably, use a school phone.
- Staff will only use school provided equipment (not personal devices):
  - to take photos or videos of pupils in line with our image use policy.
  - to work directly with pupils during lessons/educational activities.
  - to communicate with parents/carers.

- Where remote learning activities take place, staff will use school provided equipment. If this is not available, staff will only use personal devices with prior approval from the DSL/headteacher, following a formal risk assessment. Staff will follow clear guidance outlined in the Acceptable Use Policy and/or remote learning AUP.

- If a member of staff breaches our policy, action will be taken in line with our staff behaviour policy/code of conduct, child protection and/or complaints policy.

- If a member of staff is thought to have illegal content saved or stored on a personal mobile or other device or have committed a criminal offence using a personal device or mobile phone, the police will be contacted, and the LADO (Local Authority Designated Officer) will be informed in line with our staff behaviour/allegations/child protection policy.

9.4 Student use of mobile and smart technology

- Pupils will be educated regarding the safe and appropriate use of mobile and smart technology, including mobile phones and personal devices, and will be made aware of behaviour expectations and consequences for policy breaches.

- Safe and appropriate use of mobile and smart technology will be taught to pupils as part of an embedded and progressive safeguarding education approach using age-appropriate sites and resources. Further information is contained within our child protection, PHSE/RSE and Computing and Acceptable Use policy and relevant specific curriculum policies**.**

- All pupils must hand in their personal mobile or smart technology to their class teacher at the beginning of the day, this will then be returned to them at the end of the day.

- If a pupil needs to contact their parents or carers whilst on site, they will be allowed to use a school phone.
  - Parents are advised to contact their child via the school office; exceptions may be permitted on a case-by-case basis, as approved by the DSL/headteacher.

- If a pupil requires access to personal mobile or smart technology devices in exceptional circumstances, for example medical assistance and monitoring, this will be discussed with the DSL/headteacher prior to use being permitted.
  - Any arrangements regarding access to personal devices in exceptional circumstances will be documented and recorded by the school.

- Any specific agreements and expectations (including sanctions for misuse) will be provided in writing and agreed by the learner and their parents carers before use is permitted.

- Where pupils' personal mobile or smart technology devices are used when learning at home, this will be in accordance with our Acceptable Use Policy and/or Remote Learning AUP.

- Personal mobile or smart technology devices must not be taken into examinations. pupils found in possession of a mobile phone or personal device which facilitates communication or internet access during an exam will be reported to the appropriate examining body. This may result in the withdrawal from either that examination or all examinations.

9.5 Searching, screening and confiscation of electronic devices (in conjunction with Behaviour policy)

- Electronic devices, including mobile phones, can contain files or data which relate to an offence, or which may cause harm to another person. This includes, but is not limited to, indecent images of children, pornography, abusive messages, images or videos, or evidence relating to suspected criminal behaviour.

- Where there are any concerns regarding pupils use of mobile or smart technology or policy breaches, they will be dealt with in accordance with our existing policies, including anti-bullying, child protection, online safety and behaviour.

- Staff may confiscate a pupils personal mobile or smart technology device if they believe it is being used to contravene our child protection or behaviour policy.

- Personal mobile or smart technology devices that have been confiscated will be held in a secure place and released to parents/carers.

- Where a concern involves a potentially indecent image or video of a child, staff will respond in line with our child protection policy and will confiscate devices, avoid looking at any content, and refer the incident to the Designated Safeguarding Lead (or deputy) urgently as they will be most appropriate person to respond.

- If there is suspicion that data or files on a pupils personal mobile or smart technology device may be illegal, or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation

- If deemed to be necessary and appropriate, searches of personal mobile or smart technology devices may be carried out in accordance with our behaviour policy and the DfE 'Searching, Screening and Confiscation' guidance.

- Staff will respond in line with our child protection policy and follow the most appropriate safeguarding response if they find images, data or files on a pupils electronic device that they reasonably suspect are

likely to put a person at risk.

- The Designated Safeguarding Lead (or deputy) will always be informed of any searching incidents where authorised members of staff have reasonable grounds to suspect a student was in possession of prohibited items, as identified in our behaviour policy.

- The Designated Safeguarding Lead (or deputy) will be involved without delay if staff believe a search of a pupils personal mobile or smart technology device has revealed a safeguarding risk.

- In exceptional circumstances and in accordance with our behaviour policy and the DfE 'Searching, Screening and Confiscation' guidance, the DSL/headteacher or authorised members of staff may examine or erase data or files if there is a good reason to do so.
    - In determining whether there is a 'good reason' to examine images, data or files, the DSL/headteacher or an authorised member of staff will need to reasonably suspect that the images, data or files on the device has been, or could be used, to cause harm, undermine the safe environment of the school and disrupt teaching, or be used to commit an offence.
    - In determining whether there is a 'good reason' to erase any images, data or files from the device, the member of staff should consider whether the material found may constitute evidence relating to a suspected offence. In those instances, the data or files should not be deleted, and the device must be handed to the police as soon as it is reasonably practicable.
    - If the data or files are not suspected to be evidence in relation to an offence, the DSL/headteacher or an authorised member of staff may delete the images, data or files if the continued existence of the data or file is likely to continue to cause harm to any person and the pupil and/or the parent refuses to delete the data or files themselves.

- If the DSL/headteacher or a member of staff finds any data or files that they suspect might constitute a specified offence, they will be delivered to the police as soon as is reasonably practicable.

9.6 Visitors' use of mobile and smart technology

- Parents/carers and visitors, including volunteers and contractors, are expected to ensure that phones are kept silenced and out of sight.

- Visitors, including volunteers and contractors, who are on site for regular or extended periods of time are expected to use personal mobile or smart technology device in accordance with our acceptable use of technology policy and other associated policies, including child protection.

- If visitors require access to personal mobile or smart technology device, for example when working with pupils as part of multi-agency activity, this will be discussed with the DSL/headteacher prior to use being permitted.
    - In the event of agreed visitor access to mobile/smart technology within school, the visitor will be given a GUEST wi-fi code which does not allow access to the school network.

- Members of staff are expected to challenge visitors if they have concerns about their use of mobile and smart technology and will inform the DSL/headteacher of any breaches of our policy.

9. Responding to Online Risks and/or Policy Breaches

- 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.
    - are informed of the need to report policy breaches or concerns in line with existing school policies and procedures. This is included in the Induction package.
    - will respect confidentiality and the need to follow the official procedures for reporting concerns.
    - will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.
    - will be made aware of how the school will monitor policy compliance. We believe in staff training and the use of AUPs for the community.

- If appropriate, after any investigations are completed, the DSL and leadership staff will debrief, identify lessons learnt and implement any policy or curriculum changes, as required.

- If we are unsure how to proceed with an incident or concern, the DSL/headteacher will seek advice from the local authority or other agency in accordance with our child protection policy i.e. Education Safeguarding Service (link: Home - Kent Safeguarding Children Multi-Agency Partnership (kscmp.org.uk))

- Where there is a concern that illegal activity has taken place, we will contact the police using 101, or 999 if there is immediate danger or risk of harm.

- If information relating to a specific incident or a concern needs to be shared beyond our community, for example if other local schools are involved or the wider public may be at risk, the DSL /headteacher will speak with the police and the Local Authority first, to ensure that potential criminal or child protection investigations are not compromised. Home - Kent Safeguarding Children Multi-Agency Partnership (kscmp.org.uk)

10.1 Concerns about student online behaviour and/or welfare

- Whitfield Aspen recognises that an initial disclosure to a trusted adult may only be the first incident reported, rather than representative of a singular incident and that trauma can impact memory, so children may not be able to recall all details or timeline of abuse. All staff will be aware certain children may face additional barriers to telling someone, for example because of their vulnerability, disability, sex, ethnicity, and/or sexual orientation.

- All concerns about pupils will be responded to and recorded in line with our child protection policy:
    - The DSL will be informed of all online safety concerns involving safeguarding or child protection risks in line with our child protection policy.
    - The DSL will ensure that online safety concerns are escalated and reported to relevant partner agencies in line with local policies and procedures.

- Abuse that occurs online and/or offsite will not be dismissed or downplayed; concerns will be treated equally seriously and in line with relevant policies/procedures, for example anti-bullying, behaviour,

child protection, online safety.

- Whitfield Aspen recognises that the law is in place to protect children and young people rather than criminalise them, and this will be explained in such a way to pupils that avoids alarming or distressing them.

- Appropriate sanctions and/or pastoral/welfare support will be implemented and/or offered to pupils as appropriate. Civil or legal action will be taken if necessary.
- We will inform parents/carers of online safety incidents or concerns involving their child, as and when required.

10.2 Concerns about staff online behaviour and/or welfare

- Any complaint about staff misuse will be managed in accordance with our allegations against staff policy/staff code of conduct/behaviour policy.

- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer) via the Education Safeguarding Service, link Home - Kent Safeguarding Children Multi-Agency Partnership (kscmp.org.uk).

- Where appropriate, welfare support will be offered, and where necessary, disciplinary, civil and/or legal action will be taken in accordance with our staff code of conduct.

10.3 Concerns about parent/carer online behaviour and/or welfare

- Concerns regarding parents/carers behaviour and/or welfare online will be reported to the DSL/headteacher and/or DSL and dealt with in line with existing policies, including but not limited to child protection, anti-bullying, complaints, allegations against staff, home-school agreements, acceptable use of technology and behaviour policy.
- Where appropriate, welfare support will be offered, and where necessary, civil and/or legal action may be taken.

10. Procedures for responding to specific online concerns

11.1 Online child-on-child abuse

- Whitfield Aspen recognises that whilst risks can be posed by unknown individuals or adults online, pupils can also abuse their peers; all online child-on-child abuse concerns will be responded to in line with our child protection and behaviour policies.

- We recognise that online child-on-child abuse can take many forms, including but not limited to:
  - bullying, including cyberbullying, prejudice-based and discriminatory bullying
  - abuse in intimate personal relationships between peers
  - physical abuse, this may include an online element which facilitates, threatens and/or encourages physical abuse
  - sexual violence and sexual harassment, which may include an online element which facilitates, threatens and/or encourages sexual violence
  - consensual and non-consensual sharing of nudes and semi-nude images and/or videos (also known as 'sexting' or 'youth produced sexual imagery')
  - causing someone to engage in sexual activity without consent, such as forcing someone to strip, touch themselves sexually, or to engage in sexual activity with a third party
  - upskirting (which is a criminal offence), which typically involves taking a picture under a person's clothing without their permission, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress or alarm
  - initiation/hazing type violence and rituals.

- Whitfield Aspen adopts a zero-tolerance approach to child-on-child abuse. We believe that abuse is abuse and it will never be tolerated or dismissed as "just banter", "just having a laugh", "part of growing up" or "boys being boys"; this can lead to a culture of unacceptable behaviours and can create an unsafe environment for children and a culture that normalises abuse, which can prevent children from coming forward to report it.

- Whitfield Aspen believes that all staff have a role to play in challenging inappropriate online behaviours between children. Staff recognise that some online child-on-child abuse issues may be affected by gender, age, ability and culture of those involved.

- Whitfield Aspen recognises that even if there are no reported cases of online child-on-child abuse, such abuse is still likely to be taking place and it may be the case that it is just not being reported. As such, it is important that staff speak to the DSL (or deputy) about any concerns regarding online child-on-child abuse.

- Concerns about child-on-child abuse taking place online offsite will be responded to as part of a partnership approach with pupils' and parents/carers; concerns will be recorded and responded to in line with existing appropriate policies, for example anti-bullying, acceptable use, behaviour and child protection policies.

- Whitfield Aspen want children to feel able to confidently report abuse and know their concerns will be treated seriously. All allegations of online child-on-child abuse will be reported to the DSL and will be recorded, investigated, and dealt with in line with associated policies, including child protection, anti-

bullying and behaviour. Pupils who experience abuse will be offered appropriate support, regardless of where the abuse takes place.

11.1.1 Child on child online sexual violence and sexual harassment

- When responding to concerns relating to online child on child sexual violence or harassment, Whitfield Aspen will follow the guidance outlined in Part Five of KCSIE.

- Online sexual violence and sexual harassment exists on a continuum and may overlap with offline behaviours; it is never acceptable. Abuse that occurs online will not be downplayed and will be treated equally seriously.

- All victims of online sexual violence or sexual harassment will be reassured that they are being taken seriously and that they will be supported and kept safe. A victim will never be given the impression that they are creating a problem by reporting online sexual violence or sexual harassment or be made to feel ashamed for making a report.

- Whitfield Aspen recognises that sexual violence and sexual harassment between children can take place online. Examples may include:
    - consensual and non-consensual sharing of nude and semi-nude images and videos
    - sharing of unwanted explicit content
    - ‘upskirting’ (which is a criminal offence and typically involves taking a picture under a person’s clothing without their permission, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress or alarm)
    - sexualised online bullying
    - unwanted sexual comments and messages, including, on social media
    - sexual exploitation, coercion and threats.

- Whitfield Aspen recognises that sexual violence and sexual harassment occurring online (either in isolation or in connection to face to face incidents) can introduce a number of complex factors. These include the potential for the incident to take place across a number of social media platforms and services, and for things to move from platform to platform online.
- Whitfield Aspen 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.

- Whitfield Aspen 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 and the support available, by implementing a range of age and ability appropriate educational methods as part of our curriculum.

- When there has been a report of online sexual violence or harassment, the DSL will make an immediate risk and needs assessment which will be considered on a case-by-case basis which explores how best to support and protect the victim and the alleged perpetrator, and any other children involved/impacted.
    - The risk and needs assessment will be recorded and kept under review and will consider the victim (especially their protection and support), the alleged perpetrator, and all other children and staff and any actions that are required to protect them.

- Reports will initially be managed internally by the DSL, and where necessary will be referred to Children's Social Care and/or the police.
- The decision making and required action taken will vary on a case by case basis but will be informed by the wishes of the victim, the nature of the alleged incident (including whether a crime may have been committed), the ages and developmental stages of the children involved, any power imbalance, if the alleged incident is a one-off or a sustained pattern of abuse, if there are any ongoing risks to the victim, other children, or staff, and any other related issues or wider context.
- If content is contained on pupils personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.

- Following an immediate risk assessment, the school will:
  - provide the necessary safeguards and support for all pupils involved, such as implementing safety plans, offering advice on blocking, reporting and removing online content, and providing appropriate counselling/pastoral support.
  - inform parents/carers for all children involved about the incident and how it is being managed and provide support and signposting, as appropriate, unless to do so would place a child at risk of significant harm.
  - if the concern involves children and young people at a different educational school, the DSL will work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
    - If a criminal offence has been committed, the DSL will discuss this with the police first to ensure that investigations are not compromised.
  - review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

- Whitfield Aspen recognises that internet brings the potential for the impact of any concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities. Whitfield Aspen also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.

11.1.2 Nude or semi-nude image sharing

- Whitfield Aspen recognises that consensual and non-consensual sharing of nudes and semi-nude images and/or videos (also known as youth produced/involved sexual imagery or "sexting") is a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).

- This policy defines sharing nude or semi-nude image sharing as when a person under the age of 18:
  - creates and/or shares nude and/or semi-nude imagery (photos or videos) of themselves with a peer(s) under the age of 18.
  - shares nude and/or semi-nude imagery created by another person under the age of 18 with a peer(s) under the age of 18.
  - possesses nude and/or semi-nude imagery created by another person under the age of 18.

- When made aware of concerns regarding nude and/or semi-nude imagery, Whitfield Aspen will follow the advice as set out in the non-statutory UKCIS guidance: 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'

- Whitfield Aspen will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of creating or sharing nude or semi-nude images and sources of support, by implementing preventative approaches, via a range of age and ability appropriate educational methods. See policies PHSE/RSE/Computing.

- We will respond to concerns regarding nude or semi-nude image sharing, regardless of whether the incident took place on site or using school provided or personal equipment.

- When made aware of concerns involving consensual and non-consensual sharing of nudes and semi-nude images and/or videos by children, staff are advised to:
    - Report any concerns to the DSL immediately.
    - Never view, copy, print, share, forward, store or save the imagery, or ask a child to share or download it – this may be illegal. If staff have already inadvertently viewed imagery, this will be immediately reported to the DSL.
    - Not delete the imagery or ask the child to delete it.
    - Not say or do anything to blame or shame any children involved.
    - Explain to child(ren) involved that they will report the issue to the DSL and reassure them that they will receive appropriate support and help.
    - Not ask the child or children involved in the incident to disclose information regarding the imagery and not share information about the incident with other members of staff, the child(ren) involved or their, or other, parents and/or carers. This is the responsibility of the DSL.

- If made aware of an incident involving nude or semi-nude imagery, DSLs will:
    - act in accordance with our child protection policies and the relevant local procedures and in line with the UKCIS guidance.
    - carry out a risk assessment in line with the UKCIS guidance which considers the age and vulnerability of pupils involved, including the possibility of carrying out relevant checks with other agencies.
    - a referral will be made to Children's Social Care and/or the police immediately if:
        - the incident involves an adult (over 18).
        - there is reason to believe that a child has been coerced, blackmailed, or groomed, or there are concerns about their capacity to consent, for example, age of the child or they have special educational needs.
        - the image/videos involve sexual acts and a child under the age of 13, depict sexual acts which are unusual for the child's developmental stage, or are violent.
        - a child is at immediate risk of harm owing to the sharing of nudes and semi-nudes.
    - The DSL may choose to involve other agencies at any time if further information/concerns are disclosed at a later date.
    - If DSLs are unsure how to proceed, advice will be sought from the local authority via Education Safeguarding Service, link Home - Kent Safeguarding Children Multi-Agency Partnership (kscmp.org.uk)
    - Store any devices securely:
        - If content is contained on pupils personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
        - If a potentially indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.

- inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate, unless to do so would place a child at risk of significant harm.
- provide the necessary safeguards and support for pupils, such as offering counselling or pastoral support.
- implement sanctions where necessary and appropriate in accordance with our behaviour policy but taking care not to further traumatise victims where possible.
- consider the deletion of images in accordance with the UKCIS guidance.
    - Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved and are sure that to do so would not place a child at risk or compromise an investigation.
    - Pupils will be supported in accessing the Childline 'Report Remove' tool where necessary: Report Remove Tool for nude images.
- review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

- We will not:
    - view any imagery, unless there is no other option, or there is a clear safeguarding need or reason to do so. If it is deemed necessary, the imagery will only be viewed where possible by the DSL in line with the national UKCIS guidance, and any decision making will be clearly documented.
    - send, share, save or make copies of content suspected to be an indecent image/video of a child and will not allow or request pupils to do so.

11.1.3 Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at Whitfield Aspen School.

- Full details of how we will respond to cyberbullying are set out in our anti-bullying policy.

11.2 Online child abuse and exploitation

- Whitfield Aspen recognises online abuse and exploitation, including sexual abuse and sexual or criminal exploitation, as a safeguarding issue and all concerns will be reported to and dealt with by the DSL, in line with our child protection policy.

- Whitfield Aspen will ensure that all members of the community are aware of online child abuse and sexual or criminal exploitation, including the possible grooming approaches which may be employed by offenders to target pupils, and understand how to respond to concerns.

- We will implement preventative approaches for online child abuse and exploitation via a range of age and ability appropriate education for pupils, staff and parents/carers (see Child Protection/ Safeguarding policy).

- We will ensure that all members of the community are aware of the support available regarding online child abuse and exploitation, both locally and nationally.

- If made aware of an incident involving online child abuse and/or exploitation, we will:

- act in accordance with our child protection policies and the relevant local safeguarding children partnership procedures.
- store any devices containing evidence securely:
  - If content is contained on pupils personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
  - If any evidence is stored on our network or devices, we will act to block access to other users and isolate the content.
- if appropriate, make a referral to Children's Social Work Service and inform the police via 101, or 999 if a student is at immediate risk.
- carry out a risk assessment which considers any vulnerabilities of pupils involved, including carrying out relevant checks with other agencies.
- inform parents/carers about the incident and how it is being managed and provide support and signposting, as appropriate.
- provide the necessary safeguards and support for pupils, such as, offering counselling or pastoral support.
- review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.

- We will respond to concerns regarding online abuse and exploitation, regardless of whether the incident took place on our premises or using school provided or personal equipment.
  - Where possible and appropriate, pupils will be involved in decision making. If appropriate, they will be empowered to report concerns themselves with support, for example if the concern relates to online sexual abuse via the National Crime Agency CEOP Command (NCA-CEOP): www.ceop.police.uk/safety-centre/

- If we are unclear whether a criminal offence has been committed, the DSL will obtain advice immediately through the Local Authority and/or police.
- We will ensure that the NCA-CEOP reporting tools are visible and available to pupils and other members of our community. www.ceop.police.uk/safety-centre/

- If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the police by the DSL.

- If members of the public or pupils at other schools or settings are believed to have been targeted, the DSL, will seek advice from the police and/or the Local Authority before sharing specific information to ensure that potential investigations are not compromised. See Link Education Safeguarding Service, Home - Kent Safeguarding Children Multi-Agency Partnership (kscmp.org.uk).

11.3 Indecent Images of Children (IIOC)

- Whitfield Aspen will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC) as appropriate.

- We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.

- We will seek to prevent accidental access to IIOC by using an Internet Service Provider (ISP) which subscribes to the Internet Watch Foundation (IWF) block list and by implementing appropriate

filtering, firewalls and anti-spam software.

- If we are unclear if a criminal offence has been committed, the DSL will obtain advice immediately through the police and/or the Local Authority via Education Safeguarding Service, link Home - Kent Safeguarding Children Multi-Agency Partnership (kscmp.org.uk).

- If made aware of IIOC, we will:
    - act in accordance with our child protection policy and the relevant local safeguarding children partnership procedures. Education Safeguarding Service, link Home - Kent Safeguarding Children Multi-Agency Partnership (kscmp.org.uk).
    - store any devices involved securely, until advice has been sought. If content is contained on pupils personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
    - immediately inform appropriate organisations, such as the IWF and police.

- If made aware that a member of staff or a pupil has been exposed to indecent images of children, we will:
    - ensure that the DSL is informed.
    - ensure that the URLs (webpage addresses), which contain the suspect images, are reported to the IWF via www.iwf.org.uk and/or police.
    - inform the police as appropriate, for example if images have been deliberately sent to or shared by pupils.
    - report concerns as appropriate to parents and carers.

- If made aware that indecent images of children have been found on school provided devices, we will:
    - ensure that the DSL is informed.
    - ensure that the URLs (webpage addresses), which contain the suspect images, are reported to the IWF via www.iwf.org.uk .
    - inform the police via 101 or 999 if there is an immediate risk of harm, and any other agencies, as appropriate.
    - only store copies of images (securely, where no one else has access to them and delete all other copies) following a written request from the police.
    - report concerns, as appropriate to parents/carers.

- If made aware that a member of staff is in possession of indecent images of children, we will:
    - ensure that the DSL/headteacher is informed in line with our managing allegations against staff policy.
    - inform the LADO and other relevant organisations, such as the police in accordance with our managing allegations against staff policy.
    - quarantine any involved school provided devices until police advice has been sought.

11.4 Online hate

- Online hate content, directed towards or posted by specific members of the community will not be tolerated at Whitfield Aspen and will be responded to in line with existing policies, including child protection, anti-bullying and behaviour.

- All members of the community will be advised to report online hate in accordance with relevant policies and procedures.

- The police will be contacted if a criminal offence is suspected.

- If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL will obtain advice through the Local Authority and/or the police. Education Safeguarding Service, link Home - Kent Safeguarding Children Multi-Agency Partnership (kscmp.org.uk).

11.5 Online radicalisation and extremism

- As per section 7 of this policy, we will take all reasonable precautions to ensure that pupils and staff are safe from terrorist and extremist material when accessing the internet on site. This is assisted through NCS who provide Fortinet (Fastvue) and antivirus protection.

- If we are concerned that a child or adult may be at risk of radicalisation online, the DSL will be informed immediately, and action will be taken in line with our child protection policy.

    - If we are concerned that a member of staff may be at risk of radicalisation online, the DSL/headteacher will be informed immediately, and action will be taken in line with our child protection and staff code of conduct policy. Education Safeguarding Service, link Home - Kent Safeguarding Children Multi-Agency Partnership (kscmp.org.uk).

11.6 Cybercrime

- Whitfield Aspen recognises that children with particular skills and interests in computing and technology may inadvertently or deliberately stray into ‘cyber-enabled’ (crimes that can happen offline but are enabled at scale and at speed online) or ‘cyber dependent’ (crimes that can be committed only by using a computer/internet enabled device) cybercrime.

- If staff are concerned that a child may be at risk of becoming involved in cyber-dependent cybercrime, the DSL will be informed, and consideration will be given to accessing local support and/or referring into the Cyber Choices programme, which aims to intervene when young people are at risk of committing, or being drawn into, low level cyber-dependent offences and divert them to a more positive use of their skills and interests.

- Where there are concerns about ‘cyber-enabled’ crime such as fraud, purchasing of illegal drugs online, child sexual abuse and exploitation, or other areas of concern such as online bullying or general online safety, they will be responded to in line with our child protection policy and other appropriate policies.

Appendix 1: e-Safety Information, Advice and Support

There is a wealth of information available to support schools, colleges and parents to keep children safe online. The following list is not exhaustive but should provide a useful starting point:

Support for parents and carers.

- Internet Matters – a not-for-profit organisation set up to empower parents and carers to keep children safe in the digital world. Their support for parents includes a range of downloadable guides covering subjects such as transition to secondary school, Vlogging & livestreaming, online gaming and cyberbullying.
- NSPCC - includes a range of resources to help parents keep children safe when they're using the internet, social networks, apps, games and more.
- Parent Info - from CEOP and Parent Zone, Parent Info is a website for parents covering all of the issues amplified by the internet. It is a free service which helps schools engage parents with expert safety advice, endorsed by the National Crime Agency's CEOP command. This website provides expert information across a range of online harms.
- Parent Zone - offers a range of resources for families, to help them meet the challenges of the digital age, including parent guides on the latest digital trends and platforms.
- Common Sense Media - Independent reviews, age ratings, & other information about all types of media including games, apps, films and books.
- Let's Talk About It has advice for parents and carers to keep children safe from online radicalisation.
- Childnet offers a toolkit to support parents and carers of children of any age to start discussions about their online life, to set boundaries around online behaviour and technology use, and to find out where to get more help and support
- London Grid for Learning has support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online

Support for children and young people

- BBC Own It – Support for young people to take control of their online life, including help and advice, skills and inspiration on topics such as friendships and bullying, safety and selfesteem. Free app available.
- Childline – includes information for pupils on sexting, gaming, grooming, bullying, porn, relationships.
- Think U Know – age appropriate advice for staying safe when using a tablet, mobile phone or computer.
- Disrespect Nobody - Home Office advice on healthy relationships, including sexting and pornography

Support and Resources for Schools: Government Guidance

- Keeping Children Safe in Education - Statutory guidance for schools and colleges on safeguarding children and safer recruitment.
- Teaching online safety in schools - DfE advice outlining how schools can ensure their pupils understand how to stay safe and behave online as part of existing curriculum requirements.

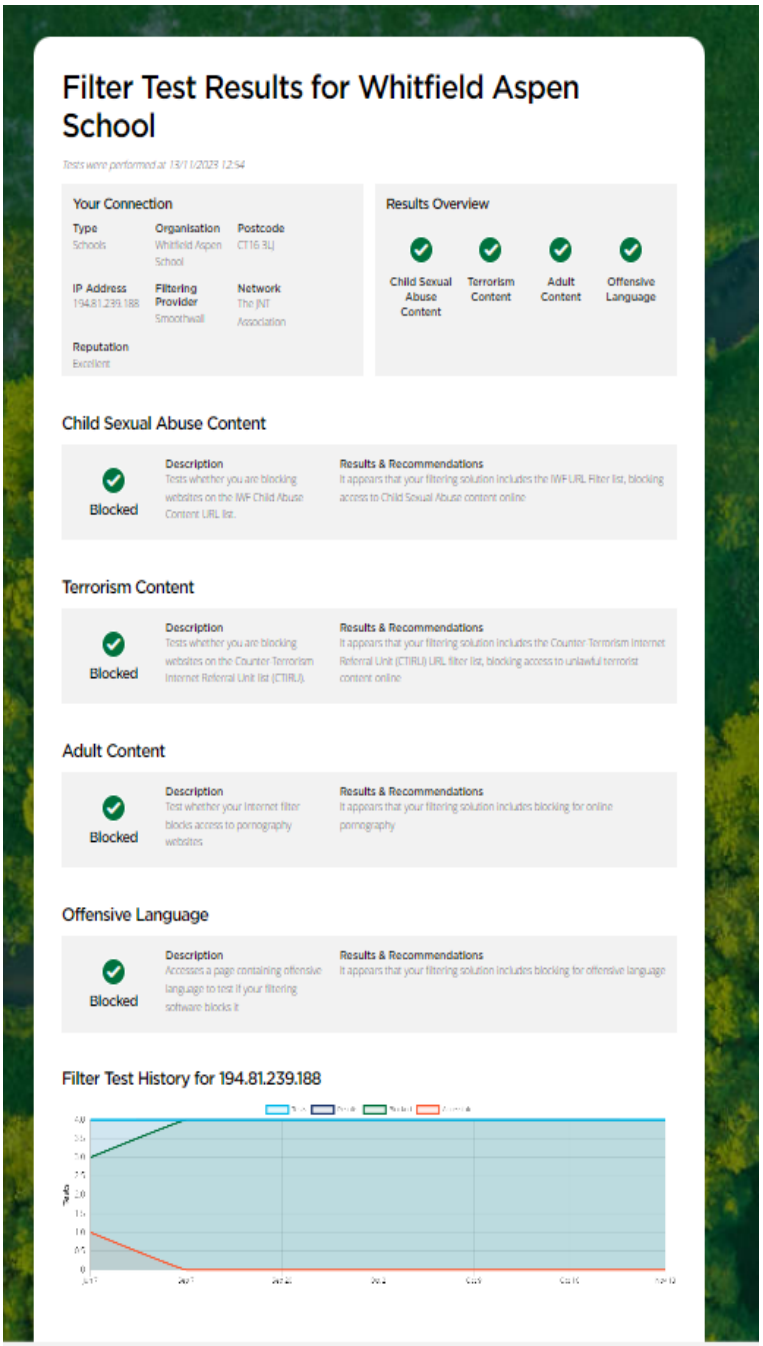
- Behaviour and discipline in schools - Guidance for school leaders and staff on developing a school behaviour policy, and a checklist of actions to take to encourage good behaviour.
- Searching, screening and confiscation at school - Guidance explaining the powers schools have to screen and search pupils, and to confiscate items they find.
- educateagainsthate - Practical advice for parents, teachers and governors on protecting children from extremism and radicalisation.
- The use of social media for online radicalisation - A briefing note for schools on how social media is used to encourage travel to Syria and Iraq.
- CEOP Think U Know Programme: Online safety education programme from the National Crime Agency's CEOP Command which aims to safeguard children from sexual abuse and exploitation. Education resources and online advice for children aged 4 – 18, expert and support and professional development for the children's workforce. Signposts to the NCA's Click CEOP service for children to report concerns related to sexual abuse.
- National Centre for Computing Education (NCCE) has been set up to support the teaching of computing education throughout schools and colleges in England, giving teachers the subject knowledge and skills to establish computing as a core part of the curriculum. To help primary and secondary schools teach the safety and security aspects of the National Curriculum Computing Programme of Study, the National Centre for Computing Education's resource repository and professional development courses cover objectives from the Education for Connected World framework. The resource repository's lesson plans will include links to the framework, as well as specific activities for non-specialist teachers.
- UK Council for Internet Safety - The UK Council for Internet Safety expands the scope of the UK Council for Child Internet Safety to achieve a safer online experience for all users, particularly groups who suffer disproportionate harms. The website has useful resources for schools and parents to help keep children safe online including: Education for a Connected World – a framework describes the Digital knowledge and skills that children and young people should have the opportunity to develop at different ages and stages of their lives. It highlights what a child should know in terms of current online technology, its influence on behaviour and development, and what skills they need to be able to navigate it.
- UK Chief Medical Officers' advice for parents and carers on children and young people's screen and social media use, published February 2019.

National Organisations: Support, Resources and Training for Schools

- National Online Safety – Specialist online safety training courses for school staff, parents and children along with resources for use in the classroom.
- The Anti-Bullying Alliance - A coalition of organisations and individuals, working together to stop bullying and create safer environments in which children and young people can live, grow, play and learn. Their website includes a range of tools and resources to support schools prevent and tackle cyberbullying.
- Childnet - a children's charity and has a wide range of practical resources freely available, covering all online safety issues, and which are available for teachers working with children of all ages, including children with SEN.
- The Diana Award – a charity running a number of different projects aimed at reducing bullying in schools. Their resource section has information to help schools tackle cyberbullying along with resources from their Be Strong Online Ambassador programme – a peer-led initiative which aims to empower young people to increase the digital resilience of their peers.

- DotCom Digital - a free resource for schools, created by children with Essex Police and the National Police Chief Council Lead for Internet Intelligence and Investigations, to be launched October 2019. The resource aims to prevent young people becoming victims of online grooming, radicalisation, exploitation and bullying by giving them the confidence to recognise warning signs and reach out to an adult for help.
- The Hopes and Streams report by London Grid for Learning has themed chapters that include links to online resources and ideas for tackling the issues raised.
- Internet Matters – a not-for-profit organisation set up to empower parents and carers to keep children safe in the digital world, they also have a dedicated section of their website for professionals which includes resources to support staff training, whole school programmes and policies and a parent pack to help schools engage with parents about online safety.
- Internet Watch Foundation – an internet hotline for the public and IT professionals to report potentially criminal online content, including child sexual abuse images online.
- NSPCC learning – includes a range of safeguarding and child protection teaching resources, advice and training for schools and colleges.
- Parent Zone's dedicated school zone - includes a range of resources to support teachers educate their pupils on how to stay safe online, what to do if they find themselves in an uncomfortable situation and how to build their digital resilience.
- PSHE Association - the national body for Personal, Social, Health and Economic (PSHE) education. Their programme of study for PSHE education aims to develop skills and attributes such as resilience, self-esteem, risk-management, team working and critical thinking. They also have many guides about how to teach specific topics.
- UK Safer Internet Centre –a partnership between Childnet International, Internet Watch Foundation and SWGfL to promote the safe and responsible use of technology for young people. Their website includes a range of practical resources and support for schools including: 360 degree safe - a free to use self-review tool for schools to assess their wider online safety policy and practice. A Helpline – This helpline was established to support those working with children across the UK with online safety issues. Operated by SWGfL, it can be contacted at 0344 381 4772 and helpline@saferinternet.org.uk. Safer Internet Day - The UK Safer Internet Centre organise Safer Internet Day for the UK and each year develops a range of materials from assemblies to lesson plans, posters to quizzes, for each Key Stage, to address a key online safety issue.
- Be Internet Legends - Be Internet Legends from Google and Parentzone a free internet safety curriculum with PSHE accredited lesson plans and teaching resources for Key Stage 2 pupils.

Appendix 2: DfE Filtering and Monitoring standards



Filter Test Results for Whitfield Aspen School

Tests were performed at 13/11/2023 12:54

Your Connection

Type: Schools
Organisation: Whitfield Aspen School
Postcode: CT16 3LJ
IP Address: 194.81.239.188
Filtering Provider: Smoothwall
Network: The JNT Association
Reputation: Excellent

Results Overview

Child Sexual Abuse Content
Terrorism Content
Adult Content
Offensive Language

Child Sexual Abuse Content

Blocked

Description: Tests whether you are blocking websites on the IWF Child Abuse Content URL list.

Results & Recommendations: It appears that your filtering solution includes the IWF URL filter list, blocking access to Child Sexual Abuse content online

Terrorism Content

Blocked

Description: Tests whether you are blocking websites on the Counter Terrorism Internet Referral Unit list (CTIRU).

Results & Recommendations: It appears that your filtering solution includes the Counter Terrorism Internet Referral Unit (CTIRU) URL filter list, blocking access to unlawful terrorist content online

Adult Content

Blocked

Description: Test whether your internet filter blocks access to pornography websites

Results & Recommendations: It appears that your filtering solution includes blocking for online pornography

Offensive Language

Blocked

Description: Accesses a page containing offensive language to test if your filtering software blocks it

Results & Recommendations: It appears that your filtering solution includes blocking for offensive language

Filter Test History for 194.81.239.188

Appendix 3: Acceptable Use of Technology Policy (AUP (Acceptable Use Policy)) Staff including Visitors and Volunteers

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use Whitfield Aspen School IT systems in a professional, lawful, and ethical manner. To ensure that members of staff understand their professional responsibilities when using technology and provide appropriate curriculum opportunities for pupils, they are asked to read and sign the staff Acceptable Use of Technology Policy (AUP).

Our AUP is not intended to unduly limit the ways in which members of staff teach or use technology professionally, or indeed how they use the internet personally, however the AUP will help ensure that all staff understand Whitfield Aspen School name expectations regarding safe and responsible technology use and can manage the potential risks posed. The AUP will also help to ensure that Whitfield Aspen School systems are protected from any accidental or deliberate misuse which could put the safety and security of our systems or members of the community at risk.

Policy scope

1. I understand that this Acceptable Use of Technology Policy (AUP) applies to my use of technology systems and services, either provided to me by the Whitfield Aspen School or accessed by me as part of my role within Whitfield Aspen School name, professionally and personally, both on and offsite. This may include my use of devices such as laptops, mobile phones, tablets, digital cameras, as well as IT systems and networks, email. data and data storage, remote learning systems and communication technologies**.**

2. I understand that Whitfield Aspen School name Acceptable Use of Technology Policy (AUP) should be read and followed in line with the Whitfield Aspen School child protection/online safety policy, staff behaviour policy/code of conduct.

3. I am aware that this AUP does not provide an exhaustive list; all staff should ensure that technology use is consistent with the Whitfield Aspen School ethos, Whitfield Aspen School staff behaviour and safeguarding policies, national and local education and child protection guidance, and the law.

Use of Whitfield Aspen School devices and systems

4. I will only use the equipment and internet services provided to me by the Whitfield Aspen School for example Whitfield Aspen School provided laptops, tablets, mobile phones, and internet access, when working with children from other establishments and our own pupils.

5. I understand that any equipment and internet services provided by my workplace is intended for education purposes and/or professional use and should only be accessed by members of staff. Reasonable personal use of setting IT systems and/or devices by staff is allowed; These devices

are still only for home internet with the usage of what is approved in the school by Fortinet (Fastvue). These devices can be considered as beneficial to the development of staff IT skills and can enable staff to maintain a positive work-life balance. However, this is at the setting's discretion and can be revoked at any time. Leaders should make informed decisions and be able to evidence their decision making.

6. Where I deliver or support remote/online learning, I will comply with the Whitfield Aspen School online learning.

Data and system security

7. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or securing/locking access.
    - I will use a 'strong' password to access Whitfield Aspen School systems. A strong password has numbers, letters, and symbols, with 8 or more characters.
    - I will protect the devices in my care from unapproved access or theft.
    - Not leaving devices visible or unsupervised in public places.
    - For insurance purpose device to be in the car boot.

8. I will respect Whitfield Aspen School system security and will not disclose my password or security information to others.

9. I will not open any hyperlinks or attachments in emails unless they are from a known and trusted source. If I have any concerns about email content sent to me, I will report them to the IT system manager or Headteacher.

10. I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the IT system manager.

11. I will ensure that any personal data is kept in accordance with the Data Protection legislation, including UK (United Kingdom) GDPR (General Data Protection Regulations) in line with the Whitfield Aspen School information security policies.
    - All personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary, and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online, or accessed remotely.
    - Any data being removed from the Whitfield Aspen School site, such as via email or on memory sticks or CDs, will be suitably protected. This may include data being encrypted by a method approved by the Whitfield Aspen School.

12. I will not keep documents which contain Whitfield Aspen School related sensitive or personal information, including images, files, videos, and emails, on any personal devices, such as laptops, digital cameras, and mobile phones. Where possible, I will use the Whitfield Aspen School Office 365 to upload any work documents and files in a password protected environment or Whitfield Aspen School approved/provided VPN.

13. I will not store any personal information on the Whitfield Aspen School IT system, including Whitfield Aspen School laptops or similar device issued to members of staff, that is unrelated to Whitfield Aspen School activities, such as personal photographs, files, or financial information.

14. I will ensure that Whitfield Aspen School owned information systems are used lawfully and appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

15. I will not attempt to bypass any filtering and/or security systems put in place by the Whitfield Aspen School.

16. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the ICT Support Provider/Team/lead (named contact) as soon as possible.

17. If I have lost any Whitfield Aspen School related documents or files, I will report this to the ICT Support Provider or SLT and Whitfield Aspen School Data Protection Officer as soon as possible.

18. Any images or videos of pupils will only be used as stated in the Whitfield Aspen School Online Policy. I understand images of pupils must always be appropriate and should only be taken with Whitfield Aspen School provided equipment and only be taken/published where pupils and/or parent/carers have given explicit written consent.

Classroom practice

19. I understand that it is part of my roles and responsibilities to ensure that appropriate filtering and monitoring is implemented by Whitfield Aspen School as detailed in Online, Child protection, and AUP and as discussed with me as part of my induction and/or ongoing safeguarding and child protection staff training.

20. If there is failure in the filtering software or abuse of the filtering or monitoring systems, for example, I witness or suspect accidental or deliberate access to illegal, inappropriate, or harmful material, I will report this to the DSL (Designated Safeguarding Lead) and IT staff, in line with the Whitfield Aspen School child protection/online safety policy.

21. I am aware of the expectations relating to safe technology use in the classroom, safe remote learning, and other working spaces as listed in child protection, online safety,

22. I will promote online safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create by:
    - exploring online safety principles as part of an embedded and progressive curriculum and reinforcing safe behaviour whenever technology is used.

- creating a safe environment where pupils feel comfortable to report concerns and say what they feel, without fear of getting into trouble and/or be judged for talking about something which happened to them online.
- involving the Designated Safeguarding Lead (DSL) or a deputy as part of planning online safety lessons or activities to ensure support is in place for any pupils who may be impacted by the content.
- Informing the DSL and/or leadership team if I am teaching topics which could create unusual activity on the filtering logs, or if the filtering system is placing unreasonable restrictions on teaching, learning or administration.
- make informed decisions to ensure any online safety resources used with pupils is appropriate.

23. I will respect copyright and intellectual property rights; I will obtain appropriate permission to use content, and if videos, images, text, or music are protected, I will not copy, share, or distribute or use them.

Mobile devices and smart technology

24. I have read and understood the Whitfield Aspen School mobile and smart technology and social media in the Online Policy which addresses use by pupils and staff.

25. I will ensure that my use of mobile devices and smart technology is compatible with my professional role, does not interfere with my work duties and takes place in line with the staff behaviour policy/code of conduct and the Whitfield Aspen School mobile technology in the Online Policy.

Online communication, including use of social media

26. I will ensure that my use of communication technology, including use of social media is compatible with my professional role, does not interfere with my work duties and takes place in line with the child protection/online safety policy, staff behaviour policy/code of conduct and in line with the UK law.

27. As outlined in the staff behaviour policy/code of conduct and Whitfield Aspen School Online policy.
    - I will take appropriate steps to protect myself and my reputation, and the reputation of the Whitfield Aspen School, online when using communication technology, including the use of social media.
    - I will not discuss or share data or information relating to pupils, staff, Whitfield Aspen School business or parents/carers on social media.

28. My electronic communications with current and past pupils and parents/carers will be transparent and open to scrutiny and will only take place within clear and explicit professional boundaries.
    - I will ensure that all electronic communications take place in a professional manner via Whitfield Aspen School approved and/or provided communication channels and systems, such as a Whitfield Aspen School email address, user account or telephone number.

- I will not share any personal contact information or details with pupils, such as my personal email address or phone number.
- I will not add or accept friend requests or communications on personal social media with current or past pupils and/or their parents/carers.
- If I am approached online by a current or past pupils or parents/carers, I will not respond and will report the communication to my line manager and Designated Safeguarding Lead (DSL).
- Any pre-existing relationships or situations that compromise my ability to comply with the AUP or other relevant policies will be discussed with the DSL and/or headteacher.

Policy concerns

29. I will not upload, download, or access any materials which are illegal, such as child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act.

30. I will not attempt to access, create, transmit, display, publish or forward any material or content online that may be harmful, inappropriate, or likely to harass, cause offence, inconvenience, or needless anxiety to any other person.

31. I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of the Whitfield Aspen School into disrepute.

32. I will report and record any concerns about the welfare, safety or behaviour of pupils or parents/carers online to the DSL in line with the Whitfield Aspen School child protection policy.

33. I will report concerns about the welfare, safety, or behaviour of staff online to the headteacher, in line with Whitfield Aspen School child protection policy, the allegations against staff policy.

Policy Compliance and Breaches

34. If I have any queries or questions regarding safe and professional practise online, either in Whitfield Aspen School or off site, I will raise them with the DSL the headteacher.

35. I understand that the Whitfield Aspen School may exercise its right to monitor the use of its devices information systems to monitor policy compliance and to ensure the safety of pupils and staff. This includes monitoring all Whitfield Aspen School provided devices and Whitfield Aspen School systems and networks including Whitfield Aspen School provided internet access, whether used on or offsite and may include the interception of messages and emails sent or received via Whitfield Aspen School provided devices, systems and networks. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.

36. I understand that if the Whitfield Aspen School believe that unauthorised and/or inappropriate use of Whitfield Aspen School devices, systems and networks is taking place, the Whitfield Aspen School may invoke its disciplinary procedures as outlined in the staff behaviour policy/code of conduct.

37. I understand that if the Whitfield Aspen School believe that unprofessional or inappropriate online activity, including behaviour which could bring the Whitfield Aspen School into disrepute, is taking place online, the Whitfield Aspen School may invoke its disciplinary procedures as outlined in the staff behaviour policy/code of conduct.

38. I understand that if the Whitfield Aspen School suspects criminal offences have occurred, the police will be informed.

I have read, understood and agreed to comply with Whitfield Aspen School Staff Acceptable Use of Technology Policy when using the internet and other associated technologies, both on and off site.

Name of staff member: ……

Signed: …….....

Date (DD/MM/YY)

Appendix 4: Acceptable Use policy agreement KS1 including Early Years and Reception



We have read this with our child

Signed …….. Parent/Carer Date: ……

Appendix 5: Acceptable Use policy and agreement KS2

- understand that the Whitfield Aspen School Acceptable Use Policy will help keep me safe and happy online at home and at school.
- I know that I will be able to use the internet in Whitfield Aspen School for a variety of reasons, if I use it responsibly. However, I understand that if I do not, I may not be allowed to use the internet at Whitfield Aspen School.
- I know that being responsible means that I should not look for bad language, inappropriate images or violent or unsuitable games, and that if I accidently come across any of these, I should report it to a teacher or adult in Whitfield Aspen School, or a parent or carer at home.
- I will treat my password like my toothbrush! This means I will not share it with anyone (even my best friend), and I will log off when I have finished using the computer or device.
- I will protect myself by not telling anyone I meet online my address, my telephone number, my Whitfield Aspen School name or by sending a picture of myself without permission from a teacher or other adult.
- I will not arrange to meet anyone I have met online alone in person without talking to a trusted adult.
- If I get unpleasant, rude, or bullying emails or messages, I will report them to a teacher or other adult. I will not delete them straight away, but instead, keep them so I can show them to the person I am reporting it to.
- I will always be myself and not pretend to be anyone or anything I am not. I know that posting anonymous messages or pretending to be someone else is not allowed.
- I will always check before I download software or data from the internet. I know that information on the internet may not be reliable and it sometimes needs checking.
- If I bring in memory sticks/CDs from outside of Whitfield Aspen School, I will always give them to my teacher so they can be checked for viruses and content before opening them.
- I will be polite and sensible when I message people online and I know that sending a message is the same as having a conversation with someone. I will not be rude or hurt someone's feelings online.
- I know that I am not allowed on personal email, social networking sites or instant messaging in Whitfield Aspen School.
- If, for any reason, I need to bring a personal/smart device and/or mobile phone into Whitfield Aspen School I know that it is to be handed in to the Class Teacher as soon as I arrive in the Classroom and then collected at the end of the Whitfield Aspen School day.
- I know that all Whitfield Aspen School devices/computers and systems are monitored.
- I will tell a teacher or other adult if someone online makes me feel uncomfortable or worried when I am online using games or other websites or apps.

Signed …….. Pupil

Pupil Name …… Date ……

Appendix 6: Parent/Carer Notification Email Template

This finalised text must be distributed to families via class email accounts regarding independent travel regulations and smart technology.

Subject: Important Information: Pupil Mobile Phone Policy and Safety Guidance for Independent Walking

Dear Parents and Carers,

As part of our continuous commitment to safeguarding and online safety at Whitfield Aspen School, we are writing to clarify out policy regarding children bringing personal mobile phones or smart devices onto the school premises.

We understand that some parents of older pupils choose to provide their child with a mobile phone for safety reasons, particularly if they are permitted to walk to and from school independently.

If your child requires a mobile phone or smart device for their journey, please note the following mandatory school procedures:-

- **Daily Hand-in**: Your child must hand their personal mobile phone or smart technology device directly to their class teacher as soon as they arrive in the classroom at the start of the day.

- **Secure Storage & Return**: All devices will be stored securely by school staff throughout the day and will be returned to your child at the end of the school day.

- **On-Site Restrictions**: Pupils are not permitted to use personal mobile devices at any time while on school grounds. If a pupil needs to contact home during school hours, they will be fully supported to use a school landline phone.

- **Urgent Contact**: If you need to pass an urgent message to your child during the day, please communicate directly with the main School Office rather than attempting to message your child's personal device.

- **Prohibited Areas**: Mobile decides are strictly forbidden in sensitive zones across our site, including changing rooms, toilets, and swimming pool areas.

- **Personal Responsibility**: Please note that any electronic device brought onto school property remains the ultimate responsibility of the user. The school accepts no liability for loss, theft or physical damage.

Continued …

If your child will be bringing a device to school for their journey, please complete and return the slip below to your child's class teacher.

Thank you for your continued partnership in keeping our school community safe.

Warm regards

Jason Cook
Designated Safeguarding Lead/Headteacher

Mobile Phone Policy Acknowledgement Slip

Pupil Name: ---------- Class: ----------

[ ] I confirm that my child requires a mobile phone for safety while walking to/from school.

[ ] I have discussed the school rules regarding daily device hand-in and usage with my child.

Parent/Carer signature: …… Date: ……