MY OASIS

Therapeutic Alternative Provision

E-safety and Acceptable Use Policy

2026/2027

Date of Last review: January 2026

Date of Next review: January 2027

CHARLOTTE LOWE
PSYCHOLOGICAL SERVICES LTD

MY OASIS
THERAPEUTIC ALTERNATIVE PROVISION

www.charlottelowepsychologicalservices.co.uk

www.my-oasis.uk

Contents

Statement of Intent

At My Oasis Therapeutic Alternative Provision (TAP), an Independent Special School, we recognise that digital technology is a powerful tool for supporting teaching, learning, safeguarding and personal development. The internet and other digital technologies expand opportunities for education, creativity, collaboration, and preparing students for life in a connected world.

At the same time, we acknowledge the associated risks, which can threaten safety, well-being and learning if not carefully managed. These include:

- Exposure to harmful or inappropriate content – such as violence, pornography, extremist material or misinformation.
- Unsafe contact with others – including online grooming, exploitation, harassment or radicalisation.
- Unsafe or illegal conduct online – such as bullying, trolling, image-based abuse, sexting or attempts to bypass security systems.
- Commercial exploitation – including scams, identity theft, fraud, in-game purchases and addictive design features.
- Emerging risks – such as misuse of artificial intelligence (AI), deepfakes, misinformation, online sexual harassment, and threats to digital wellbeing (e.g., screen time, social pressures and gaming addiction).

This E-Safety and Acceptable Use Policy is designed to ensure that all students, staff, volunteers and visitors use technology safely, responsibly and respectfully. It sets out the safeguards, education, monitoring and reporting arrangements that underpin our whole-school approach to digital safety and resilience.

My Oasis is committed to:

- Providing a safe, supportive digital environment for all students, staff and volunteers.
- Embedding online safety across the curriculum, including PSHE, RSE, and Computing.
- Equipping students with the knowledge, skills and confidence to navigate the online world critically, lawfully and responsibly.
- Working in partnership with parents, carers and the wider community to promote safe, balanced and positive use of technology.
- Regularly reviewing practice, staff training and technology to respond to new and emerging online risks, in line with Keeping Children Safe in Education (KCSIE) and other statutory guidance.

Legal and Statutory Framework

This E-Safety and Online Safety Policy has been developed with due regard to relevant legislation, statutory guidance and national frameworks. It ensures that My Oasis Therapeutic Alternative Provision fulfils its duty to safeguard and promote the welfare of children, as required under education law and statutory guidance.

Legislation:
This policy reflects, but is not limited to, the following legislation:

- UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 – protecting personal data and digital privacy.
- Freedom of Information Act 2000 – ensuring transparency of school information.

- Human Rights Act 1998 – upholding the rights to privacy and freedom of expression.
- Equality Act 2010 – ensuring fair and inclusive treatment online and offline.
- Malicious Communications Act 1988 and Communications Act 2003 – criminalising offensive and harmful online communication.
- Computer Misuse Act 1990 – protecting against hacking and unauthorised access.
- Protection of Children Act 1978 – prohibiting the creation, distribution and possession of indecent images of children.
- Education Act 2002 (Section 175) – placing a duty on schools to safeguard and promote student welfare.
- Counter-Terrorism and Security Act 2015 (Prevent Duty) – requiring schools to prevent students from being drawn into terrorism or extremist activity.
- Independent School Standards Regulations 2014 (ISSRs) – requiring independent schools to have appropriate safeguarding and e-safety measures.

Statutory and Non-Statutory Guidance:

This policy also draws on the following statutory and advisory guidance:

- DfE (2025) Keeping Children Safe in Education (KCSIE) – statutory safeguarding guidance for all schools.
- DfE (2025) Updated Filtering and Monitoring Standards – setting technical expectations for online safeguarding.
- DfE (2023) Teaching Online Safety in Schools – guidance for embedding e-safety into the curriculum.
- UKCIS (2020) Education for a Connected World Framework – age-appropriate progression framework for online safety.
- UKCIS (2024) Sharing Nudes and Semi-Nudes: Advice for Education Settings – responding to incidents of image-based abuse.
- DfE (2022) Searching, Screening and Confiscation – powers to search for and seize digital devices.
- DfE (2023) Prevent Duty Guidance – updated expectations on preventing radicalisation and extremism.

Associated My Oasis Policies and Procedures

This policy should be read in conjunction with the following related school policies and procedures:

- Safeguarding and Child Protection Policy
- GDPR and Data Protection Policy
- Behaviour Policy
- Anti-Bullying Policy
- Code of Conduct
- Relationships and Sex Education (RSHE) Policy
- Personal, Social, Health and Economic Education (PSHE) Policy

Scope of the Policy

This E-Safety and Online Safety Policy applies to all members of the company/school community, including:

- Students (full-time, part-time and those attending on a short-term basis)
- Staff (teaching, support, administrative and managing staff)
- Volunteers and visitors (including governors, contractors, and external agency staff, students on placement)
- Parents and carers, where relevant to their role in supporting safe online use

Coverage

This policy applies to the use of:

- School-owned technology – including computers, laptops, tablets, interactive whiteboards, and other devices provided by My Oasis.
- Personal devices – where students, staff or visitors access the school's learning platforms and/or systems off school premises or for school-related purposes.
- School-provided internet access – including wired, wireless and remote connections.
- Digital communication systems – including email, messaging platforms, virtual classrooms, and school learning management systems.
- Remote learning technologies – including online lessons, digital platforms, and cloud-based systems used for education delivery.
- Social media and online platforms – when used in an educational context, for school communication, or where there is a direct link to the school community.

Application Beyond the School

The expectations outlined in this policy apply not only on school premises but also:

- When students are engaged in off-site learning, school trips, or residential activities.
- When students or staff are using remote access or online platforms outside normal school hours.
- Where incidents occur outside of school that impact the safety, well-being, or reputation of students, staff or the school community.

Exclusions

This policy does not cover:

- The personal, private use of technology by staff or parents/carers outside of a school-related context, unless such use impacts the safeguarding of students or the reputation of My Oasis.

Accountability

All members of the My Oasis community are expected to familiarise themselves with this policy, act in accordance with its principles, and report any online safety concerns promptly.

Roles and Responsibilities

Ensuring online safety is a shared responsibility across the whole My Oasis community. Every member of staff, student, parent, carer, governor, and visitor has a role to play in promoting safe, responsible, and respectful use of technology.

Clear lines of accountability are essential: leadership sets the strategic direction; the DSL oversees safeguarding; the PSHE Lead ensures curriculum coverage; IT staff maintain safe systems; teaching staff model good practice; students and parents engage in positive digital behaviours. Together, these responsibilities create a consistent, whole-school approach to e-safety and online safety.

Governing Body / Proprietor

- Ensure compliance with Keeping Children Safe in Education (2025) and other statutory guidance.
- Approve this policy and review it annually.
- Receive regular reports on online safety, including:
    - Filtering and monitoring performance
    - Incidents and safeguarding concerns
    - Staff training and CPD
    - Curriculum delivery (including PSHE, RSE, and Computing).
- Hold the Headteacher and DSL to account for the effective implementation of this policy.

Headteacher / Senior Leadership Team (SLT)

- Provide overall strategic leadership for online safety.
- Ensure online safety is embedded across the curriculum, including PSHE, RSHE, and Computing.
- Allocate resources (time, training, budget) to online safety.
- Ensure all staff, students, and parents are aware of reporting procedures.
- Support the DSL, PSHE Lead, IT staff, and others in delivering high-quality online safety education and safeguarding.

Designated Safeguarding Lead (DSL)

- Take lead responsibility for safeguarding, including online safety case management.
- Liaise with the PSHE Lead to ensure curriculum content reflects current and emerging risks (AI, sexting, deepfakes, online sexual harassment, scams, misinformation, radicalisation, etc.).
- Monitor incidents and online safety trends, feeding intelligence into safeguarding, PSHE, and RSHE.
- Provide advice, support, and training to staff on online safety concerns.
- Liaise with external agencies (police, CEOP, social care, LA safeguarding partners) as appropriate.
- Ensure accurate records of online safety concerns are kept and reported to SLT and governors.

PSHE Lead

- Plan, coordinate, and oversee the delivery of online safety education within the PSHE curriculum.
- Ensure lessons cover:
    1. Respectful relationships and consent
    2. Sexting and image-based abuse
    3. Harmful online challenges and trends
    4. Digital wellbeing and screen time
    5. Misinformation and fake news
    6. Safe and ethical use of AI
- Work closely with the DSL to integrate safeguarding priorities into PSHE teaching.
- Support other staff delivering PSHE with resources, training, and up-to-date guidance.
- Provide feedback to SLT and governors on online safety curriculum effectiveness.

Teaching and Support Staff

- Deliver online safety content within PSHE, RSHE, Computing, and across the wider curriculum.
- Reinforce safe and responsible use of technology in teaching and pastoral support.
- Act as positive role models in digital conduct (e.g. respecting copyright, avoiding plagiarism, using secure platforms).
- Report online safety concerns or incidents immediately to the DSL.
- Participate in training and maintain awareness of current online risks.

IT / Technical Staff

- Maintain safe and secure IT systems, filtering, and monitoring in line with DfE Filtering and Monitoring Standards (2025).
- Implement updates, patches, and security controls to reduce risk.
- Ensure age-appropriate filtering is in place without unduly impacting learning.
- Support staff and students in safe use of school devices and platforms.
- Report technical incidents with safeguarding implications to the DSL.

Students

- Participate actively in online safety education through PSHE, RSE, and Computing.
- Use technology safely, respectfully, and responsibly in line with this policy and the Acceptable Use Agreement.
- Report any concerns, abuse, or misuse immediately to a trusted adult, mentor, or the DSL.
- Support peers by promoting positive online behaviours.

Parents and Carers

- Reinforce online safety messages taught at school through discussions at home.
- Engage with school guidance, newsletters, and workshops about online risks.
- Encourage children to talk openly about their online experiences, including concerns.
- Support the school in promoting safe and responsible use of technology.

Visitors, Volunteers, and Contractors

- Must comply with the Acceptable Use Agreement when accessing school systems or devices.
- Report any safeguarding or online safety concerns to the DSL immediately.
- Use of personal devices to photograph or video students is not permitted, similar to the restriction imposed on employees.

Online Risks

My Oasis recognises that the internet and digital technologies create opportunities for learning, connection, and creativity, but also expose young people to significant risks. These risks can be understood through the **4Cs framework** (Content, Contact, Conduct, Commerce) and also include emerging and complex threats linked to technology misuse.

The 4Cs of Online Risk

- **Content risks** – exposure to illegal, harmful, or age-inappropriate material, including pornography, violence, extremist or radicalising material, misinformation, conspiracy theories, or deepfake content.
- **Contact risks** – harmful online interaction with others, such as grooming, online sexual harassment, coercion to share images, unwanted contact from adults or peers, or radicalisation attempts.
- **Conduct risks** – online behaviour that increases the likelihood of harm, including cyberbullying, sexting, trolling, hacking, sharing harmful challenges or dares, or engaging in illegal activity.
- **Commerce risks** – risks arising from online commercial pressures, such as scams, gambling-style games, financial fraud, in-app purchases, advertising and profiling, addictive design features, and exploitation of personal data.

Specific Online Risks Identified by My Oasis

- Cyberbullying and harassment, including peer-to-peer abuse, online shaming, and group exclusion.
- Sexting and image-based abuse, including deepfakes.
- Online sexual harassment such as unsolicited images, sexist language, and coercion.
- Radicalisation and extremism, including exposure to extremist content and recruitment attempts.
- Misinformation and disinformation, including fake news, conspiracy theories, and misleading AI-generated content.
- Misuse of Artificial Intelligence, including deepfakes, impersonation, plagiarism, algorithmic bias, and manipulation.
- Online challenges, trends, and hoaxes that encourage unsafe or harmful behaviour.
- Digital well-being concerns including excessive screen time, sleep disruption, online addiction, and body image pressures from social media.
- Privacy and data exploitation, such as phishing, identity theft, online scams, and loss of personal data.
- Exposure to inappropriate communities, including pro-anorexia, self-harm, or suicide-promoting content.

My Oasis ensures that students are taught how to recognise and respond to these risks (see Education and Training), and that staff, parents, and carers are equipped to identify, prevent, and report harmful online activity.

Safe and Responsible Use of the Internet

At My Oasis, promoting the safe and responsible use of the internet is central to supporting students' learning, safeguarding, and personal development. Safe and responsible use includes understanding the potential risks of online activity, following clear expectations, and using technology in ways that are respectful, lawful, and positive.

Expectations for Students

- Use all technology in a way that is safe, responsible, and respectful at all times.
- Personal technology and devices must not be brought from home. If brought, they are to be handed to a staff member for secure storage and will be returned at the end of the day. The school or the company is not responsible for any damage to personal technology and devices if brought onto the premises.
- Protect personal information and the privacy of themselves and others.
- Recognise and avoid harmful online behaviour, including cyberbullying, harassment, or illegal activity.
- Report any unsafe or suspicious online activity to a trusted adult, mentor, or the Designated Safeguarding Lead (DSL).
- Think critically about the content they view and share, including misinformation or AI-generated material.
- Maintain balance in online activity to support digital well-being.

Expectations for Staff

- Model safe, respectful, and responsible online behaviour at all times.
- Promote and reinforce online safety across teaching, pastoral care, and communications with students.
- Follow the Staff Code of Conduct regarding the use of personal and company/school technology and devices. This includes information on professional boundaries, social media use, and approved digital communication systems. Personal devices are not to be used for work purposes.
- Ensure any technology used for teaching or administrative purposes meets safety and security standards.

Expectations for Parents and Carers

- Encourage your child not to bring personal technology or electronic devices from home.
- Reinforce the importance of safe, responsible, and respectful online behaviour at home.
- Support the school's online safety messages, policies, and guidance.
- Engage in discussions with children about their online experiences and any concerns.
- Use parental controls and monitoring tools to complement learning about digital safety.

Safe Technology Practices

To maintain a secure and supportive digital environment, My Oasis:

- Implements, monitors and develops filtering and monitoring in line with DfE guidance to protect students from harmful content.
- Ensures secure access to online platforms, including remote learning and portable devices.
- Provides guidance and training for students and staff on secure password use, phishing awareness, and protecting personal data.
- Reviews and updates technology, policies, and practices regularly to respond to emerging risks.

By establishing clear expectations and safe practices, My Oasis empowers students to use the internet responsibly, enabling learning, creativity, and collaboration while minimising potential harm.

Unacceptable Internet Use

The following behaviours are strictly prohibited for both students and staff. Breaches of these rules may result in disciplinary action in line with the Behaviour Policy, Staff Code of Conduct, or Safeguarding Policy, and in some cases referral to the police or external agencies.

Use of the internet, digital devices, or AI tools to:

- Commit or facilitate illegal activities, including fraud, identity theft, hacking or copyright infringement.
- Access, create, generate, store, or share harmful or inappropriate material, including pornography, extreme violence, hate speech, discriminatory content, or material promoting self-harm, suicide, eating disorders, extremism or radicalisation.
- Create, request, share, or forward sexualised, nude, or semi-nude images or videos, including those generated or manipulated by artificial intelligence (AI deepfakes).
- Engage in online sexual harassment, including sending unwanted sexualised messages, “sextortion,” upskirting, or sharing/shaming others with intimate images.
- Use AI tools to plagiarise academic work, generate harmful or discriminatory content, or impersonate others (e.g. deepfake identities).
- Bully, harass, threaten, or intimidate others, including through social media, gaming platforms, or messaging apps.
- Attempt to bypass or disable the school’s filtering, monitoring, or security systems (e.g. using VPNs, proxies, or hotspot tethering).
- Access another person’s account, system, or data without authorisation.
- Share personal information (their own or others’) in unsafe ways, including addresses, phone numbers, financial information, or login details.
- Download, install, or run unauthorised software, apps, or executable files that could compromise security.
- Use school/company devices or networks for gambling, online trading, cryptocurrency, or financial scams.
- Use school/company devices or networks for personal or commercial purposes without permission.
- Share confidential school data, student records, or staff information without authorisation.

E-safety Control Measures

At present, My Oasis is in the process of developing its ICT provision. Currently, students have limited access to technology, and this is tightly controlled and supervised:

Current Control Measures

• Supervised Access: Students and staff use school/company devices only. When used by students, this is under direct staff supervision and strictly for educational purposes.

• Staff Laptops: Students may not access staff laptops at any time, even whilst under one-to-one supervision.

• School-Connected Devices: Students are not to use devices provided by home or host schools and are bound by My Oasis' policies.

• Immediate Response to Concerns: Any incidents of misuse or concerning behaviour are logged and reported directly to the DSL or Headteacher.

• Dedicated Student Devices: Student laptops and tablets are equipped with safeguarding controls to ensure safe use.

• Filtering and Monitoring: Robust and appropriate filtering and monitoring systems compliant with DfE Filtering and Monitoring Standards (2025) are in place to:

- Block harmful or inappropriate content, including pornography, violence, extremism, gambling, scams, and AI-generated harmful material.
- Monitor user activity and trigger alerts for concerning searches or behaviour.
- Maintain detailed logs identifying the user, device, accessed site or service, and the activity that generated the alert.

• Alerts and Escalation: Alerts are sent and/or communicated to the Facilities/IT Manager, DSL, and Headteacher. Serious incidents are escalated to relevant external agencies (e.g., Police, CEOP, IWF, LADO) when necessary.

• Incident Logging: All online safety incidents are recorded centrally, regularly reviewed by the DSL, and used to identify patterns and inform staff and student education.

• Data Handling: Monitoring data is stored securely, accessible only to authorised staff, and used solely for safeguarding or evidential purposes.

Developing Control Measures

As My Oasis expands its digital capacity, the following systems and processes will be introduced:

- Cybersecurity Standards: All school-owned devices will be encrypted, password-protected, and maintained to Cyber Essentials standards, including regular updates, malware protection, and secure backup systems.
- Annual Review: Filtering and monitoring systems will be reviewed annually, and after significant incidents, with outcomes reported to governors/proprietors for continuous improvement.

User Awareness and Education

- All students, staff, and volunteers will be made aware that technology use is subject to monitoring, in line with the Acceptable Use Policy.
- Breaches of this policy may result in disciplinary action, safeguarding referrals, and/or police involvement.
- Students will be explicitly taught about safe device use, the reasons behind filtering and monitoring, and how to report concerns.
- Staff will receive regular training on interpreting monitoring alerts, responding to incidents, and supporting students in safe technology use.

Use of Social Media

My Oasis Therapeutic Alternative Provision recognises the significant role social media plays in the lives of children, staff, parents, and the wider community. While it provides opportunities for communication, celebration of achievement and community engagement, it also carries safeguarding, wellbeing and reputational risks. This section sets out how social media will be used safely and responsibly within our school community.

1. School's Official Use of Social Media

The school may operate official social media accounts to share updates and highlight achievements. Only designated staff, authorised by the Headteacher, may manage or post on these accounts.

- All content must comply with data protection legislation; no personal information or identifiable images of students will be published without parental consent.
- Content will reflect the values of the school and uphold safeguarding responsibilities under Keeping Children Safe in Education (2025).
- Staff managing official accounts will receive guidance on safe practice, and posts will be professional, accurate, and respectful.
- The school will not engage in disputes or arguments with members of the public via social media, in line with the Complaints Policy.

2. Students' Use of Social Media

Access to social media platforms through school systems is restricted and filtered, in line with the DfE Filtering and Monitoring Standards (2025). Students may only access social media for curriculum purposes where this has been approved by the Headteacher and is directly supervised by staff.

Through the PSHE and RSHE curriculum, supported by the UKCIS Education for a Connected World framework (2020), students are taught about:

- The risks of sharing personal information or images online including long-term implications for their digital footprint.

- How online activity can affect future education and employment opportunities.
- The dangers of grooming, harassment, sexual exploitation, sextortion, and online radicalisation.
- Recognising misinformation, disinformation, and manipulated or AI-generated media.

Students must not use social media to bully, harass, intimidate, or damage the reputation of the school or its community. Misuse will be dealt with under the Behaviour Policy and, where necessary, safeguarding procedures.

3. Staff Use of Social Media

In line with the Staff Code of Conduct and statutory safeguarding guidance, staff are expected to maintain the highest standards of professionalism online.

- Staff must not communicate with students via personal social media accounts, messaging apps, or private emails.
- "Friending," "following," or otherwise connecting with students on personal accounts is prohibited.
- Staff are required to manage their privacy settings carefully and be mindful that even private posts may become public.
- Staff must not post material that could bring the school into disrepute, breach confidentiality, or conflict with safeguarding responsibilities.

Breaches of this policy will be managed under the Staff Disciplinary Policy and may be referred to the DSL, Headteacher, or the Local Authority Designated Officer where safeguarding concerns arise.

4. Parents, Carers and the Wider Community

Parents and carers are expected to engage with the school respectfully and responsibly online. Concerns should be raised through the school's complaints procedures, not through public discussion on social media.

The school reserves the right to take action where online behaviour by parents or community members:

- Harasses or bullies staff or students.
- Breaches confidentiality or data protection.
- Damages the reputation of the school.

Where appropriate, concerns will be dealt with as safeguarding issues under Keeping Children Safe in Education (2025).

5. Safeguarding and Reporting

All members of the school community are encouraged to report harmful or inappropriate social media activity.

Concerns will be recorded and addressed by the Designated Safeguarding Lead in accordance with the Child Protection and Safeguarding Policy. Where necessary, the school will escalate incidents to relevant agencies such as the police, the Internet Watch Foundation or CEOP.

Education and Training

Educating Students
At My Oasis, online safety education is fundamental to safeguarding students and promoting responsible, informed use of technology. All students, staff, and parents receive structured guidance and support to understand online risks, safe practices, and legal responsibilities.

Educating Students
Students are provided with age-appropriate online safety education throughout their time at My Oasis. This is embedded across the curriculum, including PSHE, RSHE, and Computing, and reinforced through assemblies, awareness campaigns, and themed events such as Safer Internet Day and Anti-Bullying Week.

Students will learn to:

- Recognise the **4Cs of online risk**—Content, Contact, Conduct, and Commerce—and understand strategies to mitigate them.
- Critically evaluate online information, recognising misinformation, “fake news,” conspiracy theories, and AI-generated content such as deepfakes.
- Understand legal obligations and safe behaviours, including copyright, academic integrity, sexting, image-based abuse, online sexual harassment, and illegal online activity.
- Protect their privacy and personal data, using secure passwords, appropriate privacy settings, and cautious sharing practices.
- Identify, respond to, and report cyberbullying, harassment, and coercion online.
- Develop digital resilience and wellbeing, including managing screen time, online balance, and avoiding addictive or harmful trends.
- Recognise online commercial pressures, scams, gambling-style games, in-app purchases, and manipulative advertising.
- Engage positively with peers and adults online, demonstrating respect, empathy, and responsible digital citizenship.

Student understanding is regularly assessed through discussions, activities, surveys, and student voice initiatives, ensuring that emerging risks are addressed and teaching remains relevant.

Educating Staff
Staff play a critical role in modelling safe and responsible online behaviour and reinforcing online safety throughout their teaching and interactions with students. My Oasis provides comprehensive training and ongoing professional development for all staff.

Training includes:

- Understanding emerging online risks, including sexting, image-based abuse, online sexual harassment, radicalisation, harmful AI misuse, misinformation, and challenges or hoaxes.
- Awareness of digital wellbeing issues, including screen time, social media pressures, and signs of online stress or addiction.
- Implementation of school policies and legal responsibilities, including the Staff Code of Conduct, Behaviour Policy, Data Protection Policy, and Child Protection and Safeguarding Policy.
- Practical guidance on using educational technology safely, managing filtering and monitoring tools, and responding to incidents.
- Guidance on supporting students in developing digital skills, resilience, and critical thinking.

New staff complete online safety training during induction, and all staff receive regular updates via CPD sessions, safeguarding briefings, and resources from the DSL and PSHE Lead.

Educating Parents and Carers

Parents and carers are key partners in promoting safe and responsible online behaviour outside of school. My Oasis engages families through:

- Regular newsletters and updates on emerging risks, trends, and safeguarding alerts.
- Practical resources to support discussions with children about online behaviour, privacy, consent, digital wellbeing, AI, and responsible social media use.
- Clear guidance on how to recognise and respond to cyberbullying, sexting, scams, and other online harms.

By equipping students, staff, and parents with the knowledge, skills, and confidence to navigate the online world safely, My Oasis fosters a culture of responsible digital citizenship and proactive safeguarding.

Remote Access and Portable Devices

My Oasis recognises that both students and staff may occasionally need to access the school's network and resources from outside the premises. To protect the confidentiality, integrity and availability of school data, robust security measures and systems will be in place for all remote access and portable device use.

Device Security

- All My Oasis-owned devices (laptops, tablets, mobile phones) will be encrypted and password-protected in line with the updated DfE Cyber Security Standards (2025).
- If any device is lost or stolen, encryption will prevent unauthorised access to data. Devices must be reported missing immediately to the Facilities/IT Manager and DSL.
- Staff and students must not take devices home. Use of school-owned equipment is strictly for authorised educational or professional purposes only.

- All sensitive data will be stored centrally on secure systems, reducing the need for multiple local copies or the use of removable media (USB sticks, external drives).

Device Register and Accountability

- A Device Register will be maintained by the Facilities/IT Manager to track the issue, return, and condition of all school-owned devices.
- Each entry will record:
    - The device type and serial number.
    - The staff or student assigned to the device.
    - The date of issue and return.
- Any reported faults, loss, or damage.
- Staff and students must sign to confirm receipt of the equipment, agree to the Acceptable Use and Online Safety Policies, and assume responsibility for its safe use. They must also sign in and out when they use it for each session.
- When devices, used for long-term, are returned (e.g. at the end of the school year, on leaving the school, or when no longer needed), this will be logged, inspected, and wiped by the Facilities/IT Manager. Throughout the year, unannounced and random inspections are conducted for all devices.

Use of Personal Devices

- Students and staff are not permitted to use personal devices for work/educational purposes.

Remote Access and Wi-Fi

- Remote access to the company's/school's systems will be limited, role-specific, and secured via strong authentication (e.g. passwords and two-factor authentication where appropriate).
- The school Wi-Fi network will be password-protected, regularly reviewed, and only shared with staff where required.
- Personal use of the school Wi-Fi on school devices is not permitted.
- A separate guest Wi-Fi network will be provided for visitors. This network will not allow access to printers, shared storage, or administrative systems.

Acceptable Use

- Staff and students must adhere to the school's Acceptable Use, Data Protection, and Safeguarding Policies when working remotely.
- Students are not permitted to use school-owned devices for non-educational purposes, such as social media, gaming, or streaming.
- Staff using My Oasis devices must use them exclusively for work purposes, whether on or off-site.
- All online activity on school devices is subject to monitoring, filtering, and logging.

Data Protection and Breach Management

- All staff and students must comply with UK GDPR and the Data Protection Act 2018.
- Any suspected or confirmed data breach must be reported immediately to the DSL and Data Protection Lead.

- Where required, data breaches will be recorded and reported to the ICO within statutory timescales.
- Any unauthorised disclosure of personal data by staff will be treated as a disciplinary matter under the Staff Code of Conduct and Disciplinary Policy.

Exit Procedure

- When a staff member or student leaves My Oasis permanently, all school-owned devices, accounts, and data (in any format) must be returned or deleted before their last day.
- The Device Register will be updated to confirm all devices have been returned, inspected, and data securely removed.

Incident Management & Reporting Misuse

At My Oasis, safeguarding online is everyone's responsibility. Any misuse of digital technology (whether by a student, member of staff, volunteer, contractor, or visitor) is managed in line with Keeping Children Safe in Education (2025), the Child Protection and Safeguarding Policy, the Behaviour Policy, the Anti-Bullying and Anti-Cyberbullying Policy, the Staff Code of Conduct, and relevant statutory and legal frameworks.

This section sets out the procedures for reporting, managing, and responding to incidents of misuse, along with the possible consequences.

Reporting Misuse

- Students must report harmful or unsafe online activity immediately to a trusted adult, mentor, teacher, or directly to the DSL.
- Staff, volunteers, and contractors have a duty under Keeping Children Safe in Education (2025) to report any suspected or confirmed online safety incidents directly to the DSL.
- Visitors are required to comply with the school's Acceptable Use and Safeguarding policies; any observed misuse must be reported to the DSL or a senior member of staff.
- Parents and carers are encouraged to inform the school of concerns regarding online harm that may affect their child.
- Anonymous reporting (such as worry boxes or digital forms) is available for students who feel unable to report directly.

Incident Management

- The DSL leads case management for all online safety concerns, ensuring that incidents are:
    - Recorded securely.
    - Risk-assessed (low, medium, high, immediate danger).
    - Managed proportionately, in line with safeguarding and disciplinary frameworks.
- If the incident involves illegal material or activity (such as child sexual abuse material, extreme violence, radicalisation content, or harassment), it will be reported without delay to the police, the Internet Watch Foundation (IWF), or the Counter Terrorism Internet Referral Unit (CTIRU).

- Device searches will follow DfE (2022) Searching, Screening and Confiscation Guidance. They will only be conducted by authorised staff, in the presence of a witness, and recorded.
- For peer-on-peer abuse (sexting, online harassment, cyberbullying), My Oasis will follow the UKCIS (2024) Sharing Nudes and Semi-Nudes and our Safeguarding Policy.
- Staff misconduct (e.g., breaching the Staff Code of Conduct, inappropriate online communication, failure to report, accessing illegal/inappropriate content) is referred to the Headteacher and managed under employment law, with escalation to the Local Authority Designated Officer (LADO), the Disclosure and Barring Service (DBS), or the Teaching Regulation Agency (TRA) where appropriate.

Consequences of Misuse

Consequences are applied fairly and consistently across the community, with consideration for intent, harm caused, and safeguarding risk.

For Students:

- Restorative interventions, reflection tasks, mentoring, or targeted education.
- Loss of access to school devices or platforms (temporary or permanent).
- Behaviour sanctions in line with the Behaviour Policy (detention, internal exclusion, suspension, or permanent exclusion).
- Safeguarding support and therapeutic intervention.
- Referral to police or external agencies where necessary.

For Staff, Volunteers, and Contractors:

- Verbal or written warnings, retraining, or increased supervision.
- Restriction or withdrawal of access to digital systems.
- Disciplinary action under the Staff Code of Conduct and employment procedures.
- Referral to the DBS, TRA, or professional regulators where required.
- Dismissal and, in cases involving illegal activity, referral to the police.

For Visitors:

- Immediate removal of access to school systems and devices.
- Withdrawal of permission to remain on site.
- Referral to police or other agencies for illegal activity.

Record-Keeping and Oversight

- All incidents and outcomes are logged securely in the school's safeguarding system.
- The DSL monitors patterns and provides termly reports to the Headteacher and Governing Body.
- Data from incidents informs staff training, parental guidance, and curriculum development.

Communication & Follow-Up

- Parents and carers are informed promptly of incidents involving their child unless doing so increases the risk of harm.
- Students and staff affected by online harm will receive safeguarding, pastoral, or therapeutic support.

- Learning from incidents is integrated into PSHE, RSHE, Computing, and staff training to strengthen preventative education.

Responding to Specific Online Concerns

Introduction

Digital technology provides powerful tools for communication, collaboration, and learning, but it also creates unique safeguarding challenges. Children and young people face a wide range of online risks, and these risks cannot be treated as generic or minor. Each has distinct features, potential harms, and legal implications.

It is the responsibility of My Oasis, in line with statutory guidance such as Keeping Children Safe in Education (2025) and legal duties under the Education Act 2002, the UK GDPR and Data Protection Act 2018, and the Counterterrorism and Security Act 2015 (Prevent Duty), to identify, respond to, and manage these risks effectively.

This section outlines the main categories of specific online risks recognised by the school. It is not exhaustive but represents the most prevalent threats faced by children and young people today. Each case will be managed individually and proportionately, taking into account:

- The nature and severity of the incident.
- The age and vulnerability of those involved.
- Whether the behaviour is experimental, reckless, or malicious.
- The wider safeguarding context and risks.
- Legal duties and referral thresholds to statutory agencies.

The following subsections define the risks, explain potential harms, and set the context for how My Oasis will safeguard students, staff, and the wider community.

1. Cyberbullying and Online Harassment

Definition:

Cyberbullying is the use of digital technology to deliberately intimidate, humiliate, threaten, or isolate another person. This includes sending abusive messages, spreading rumours, sharing private content without consent, exclusion from online groups, impersonation, or public shaming on social media. Cyberbullying can be peer-to-peer or adult-to-student, and may occur via messaging apps, social media, emails, or gaming platforms.

Risks:

- Emotional and Mental Health: Anxiety, depression, low self-esteem, social withdrawal, and self-harm.

- Educational Impact: Absenteeism, reduced engagement, poor performance.
- Reputational Risk: Public sharing can damage a student's or staff member's reputation.
- Legal Consequences: Criminal liability under the Malicious Communications Act 1988 or Communications Act 2003.
- Escalation Potential: Can lead to physical bullying or wider safeguarding concerns if left unaddressed.

2. Sharing Nudes and Semi-Nudes

Definition:
The sharing of sexually explicit images or videos by minors, or between minors and adults. This includes self-generated images ("sexting") and images shared without consent. It can also involve coercion or pressure from peers or adults.

Risks:
- Criminal Liability: Illegal under the Protection of Children Act 1978. Even self-generated images may result in a criminal investigation.
- Emotional Trauma: Shame, guilt, fear, and social isolation.
- Social Consequences: Stigma, bullying, and breakdown of relationships.
- Online Permanence: Once uploaded, content is difficult or impossible to remove.
- Exploitation Risk: Images may be used to coerce, groom, or blackmail victims.

3. Online Sexual Harassment and Upskirting

Definition:
Online sexual harassment includes unwanted sexual comments, sharing sexualised images, or inappropriate behaviour directed at someone online. "Upskirting" refers to taking sexualised images without consent, whether captured offline and uploaded online, or taken digitally.

Risks:
- Psychological Impact: Anxiety, trauma, and violation of dignity.
- Relationship Strain: Victims may withdraw or distrust peers/adults.
- Legal Consequences: Criminal offences under sexual offences legislation and the Malicious Communications Act 1988.
- Escalation Risk: May lead to stalking, offline abuse, or sexual exploitation.

4. Peer-on-Peer Abuse

Definition:
Harmful behaviour from one student towards another, including sexual harassment, bullying, coercion, exploitation, or physical abuse. It may occur online or offline and is recognised in KCSIE 2025 as a serious safeguarding concern.

Risks:

- Physical Harm: Risk of assault or injury.
- Mental Health: Anxiety, self-harm, or trauma.
- Educational Impact: Reduced attendance, participation, and academic outcomes.
- Criminal Implications: Some behaviours may constitute offences depending on severity and age.
- Digital Amplification: Harmful content may spread rapidly online.

5. Online Sexual Exploitation and Grooming

Definition:
Adults or older peers manipulate children online to exploit them sexually, emotionally, or financially. Grooming often occurs via social media, gaming, or messaging platforms and may involve flattery, coercion, threats, or gifts.

Risks:
- Physical and Sexual Harm: Victims may be coerced into sexual activity.
- Psychological Impact: Long-term trauma, anxiety, depression.
- Digital Vulnerability: Sharing personal information or images increases risk.
- Legal Consequences: Grooming is criminal under the Sexual Offences Act 2003 and the Protection of Children Act 1978.
- Social Risk: Damaged peer/family relationships, trust issues.

6. Radicalisation and Extremism

Definition:
Exposure to online extremist or terrorist material or attempts to manipulate young people into adopting radical ideologies. Platforms include social media, forums, chat rooms, and video-sharing sites.

Risks:
- Psychological Manipulation: Exploitation of vulnerabilities and identity crises.
- Social Isolation: Withdrawal from peers or family.
- Physical Danger: Involvement in extremist or violent activity.
- Legal Duty: Schools are legally obliged under the Prevent Duty (Counterterrorism and Security Act 2015) to protect children from radicalisation.
- Reputational Risk: Negative media attention or regulatory consequences if not addressed.

7. AI Misuse and Misinformation

Definition:
Use of artificial intelligence to create manipulated content (e.g., deepfakes), impersonations, or misleading information. Includes spreading false or harmful content for pranks, bullying, or ideological reasons.

Risks:

- Reputational Harm: False content can damage individuals or the school.
- Emotional Distress: Victims may feel violated or unsafe.
- Legal Liability: Sharing defamatory or harmful AI-generated content may breach the Malicious Communications Act 1988.
- Digital Literacy Gap: Students may struggle to tell fact from manipulation, increasing vulnerability to exploitation.

8. Cybersecurity Threats and Scams

Definition:
Attempts to gain unauthorised access, steal information, or exploit individuals or the school digitally. Includes phishing, malware, hacking, social engineering, and ransomware attacks.

Risks:

- Data Theft: Loss of sensitive student or staff data.
- School Network Compromise: Disruption of learning and records.
- Financial Loss: Fraudulent schemes or extortion.
- Psychological Impact: Stress caused by scams or threats.
- Legal Implications: Violations of the Computer Misuse Act 1990.

9. Data Breaches and Privacy Violations

Definition:
The unauthorised access, misuse, or sharing of personal or sensitive data belonging to students, staff, or families. May occur through technical failure, negligence, or malicious intent.

Risks:

- Legal Non-Compliance: Breaches may violate the UK GDPR and Data Protection Act 2018.
- Reputational Damage: Loss of trust from parents and the community.
- Emotional Harm: Victims may feel exposed, unsafe, or vulnerable.
- Financial Impact: Possible fines, compensation, or remediation costs.
- Exploitation: Stolen data may be misused for grooming, fraud, or bullying.

Data Protection & Confidentiality

At My Oasis, we recognise that safeguarding online safety is inseparable from protecting personal data and respecting confidentiality. The inappropriate handling of personal or sensitive data can expose students, staff, and the school community to significant risk, including identity theft, reputational damage, and breaches of trust.

We are committed to full compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and associated statutory guidance, including Keeping Children Safe in Education (KCSIE 2025).

Principles of Data Protection

All staff, students, volunteers, and visitors are expected to follow the seven principles of data protection as defined in Article 5 of the UK GDPR and explained by the Information Commissioner's Office (ICO):

1. Lawfulness, Fairness and Transparency – personal data will be processed legally, openly, and fairly.
2. Purpose Limitation – data will only be collected for specific, explicit, and legitimate purposes.
3. Data Minimisation – only the minimum data necessary for safeguarding, education, or administrative purposes will be collected.
4. Accuracy – personal data will be kept up-to-date and accurate, with errors corrected without delay.
5. Storage Limitation – data will only be retained for as long as necessary, in line with statutory retention schedules.
6. Integrity and Confidentiality (Security) – personal data will be kept secure and protected against unlawful access, loss, or damage.
7. Accountability – My Oasis TAP will demonstrate compliance through clear policies, staff training, monitoring, and record-keeping.

These principles are legally binding and provide the framework for all handling of personal information within the school.

Confidentiality in Practice

- Safeguarding First – Confidentiality will never prevent staff from sharing a safeguarding concern with the Designated Safeguarding Lead (DSL) or external agencies, in line with statutory duties.
- Secure Communication – Personal and sensitive data will only be shared through secure systems (e.g., encrypted email, password-protected documents) and never through unauthorised platforms or personal devices.
- Professional Boundaries – Staff must not discuss students' personal details or online safety concerns outside professional contexts or with unauthorised individuals.
- Anonymisation – Where possible, data will be anonymised when used for monitoring, reporting, or training purposes.
- Confidential Conversations – Students will be encouraged to speak openly about online concerns, with reassurance that information will only be shared on a "need-to-know" basis to keep them safe.

Responsibilities

- Headteacher/SLT – overall accountability for compliance with UK GDPR and the Data Protection Act 2018.
- Data Protection Officer (DPO) – ensures the school meets statutory obligations, advises on safe data handling, and reports breaches where required.
- All Staff & Volunteers – must complete regular data protection training and handle personal information securely at all times.

- IT/Technical Provider – ensures that technical systems, filtering, monitoring, and storage solutions meet required security standards.

Data Security Measures

- All school devices will be password-protected, encrypted where appropriate, and set to auto-lock after periods of inactivity.
- Cloud storage solutions and online platforms will comply with GDPR and have robust security arrangements.
- Personal data will not be stored on personal devices or unencrypted portable media (e.g., USB sticks).
- Filtering and monitoring systems will log access to sensitive data, with alerts for unauthorised attempts.
- All data breaches or near-misses must be reported immediately to the DPO and DSL for investigation and, where necessary, reported to the Information Commissioner's Office (ICO) within 72 hours.

Monitoring and Review

At My Oasis, we recognise that online safety is a dynamic and evolving area of safeguarding. Risks change rapidly with technological developments, and our policy and practice must remain current, effective, and evidence-based. For this reason, monitoring and review are embedded into our safeguarding culture.

Ongoing Monitoring

- Filtering and Monitoring Systems – Our IT provider maintains filtering and monitoring in line with DfE Filtering and Monitoring Standards (2023). Logs of activity are regularly reviewed to detect unsafe or inappropriate use.
- Unannounced and random inspections are conducted on all devices throughout the year.
- Incident Reporting – All online safety incidents, including misuse by students, staff, volunteers, or visitors, are recorded and reviewed by the DSL. Patterns or trends are reported to SLT and governors/proprietors.
- Curriculum Impact – The PSHE Lead, supported by the DSL, reviews how effectively online safety is embedded across PSHE, RSHE, Computing, and wider teaching. Student voice activities are used to evaluate understanding and identify emerging risks.
- Staff Practice – Staff compliance with this policy alongside the Code of Conduct and safeguarding expectations is monitored through line management, safeguarding audits, and training evaluations.
- Parental Engagement – Feedback from parents and carers on workshops, newsletters, and guidance is used to adapt and strengthen outreach on online safety.

Annual Review

- The DSL will produce an annual online safety report for SLT and the governing body/proprietor, covering incidents, training, curriculum delivery, and technology systems.
- The Headteacher and DSL will review this policy at least annually, or sooner if significant changes in legislation, statutory guidance, or local/national risks occur.

- The governing body/proprietor will approve this policy annually and ensure that updates reflect compliance with Keeping Children Safe in Education (2024), Working Together to Safeguard Children (2023), and DfE Online Safety Guidance.
- Student, staff, and parent feedback will be incorporated into the annual review to ensure the policy remains responsive to the needs of the school community.

Continuous Improvement

- Training, resources, and filtering/monitoring systems will be updated promptly in response to new and emerging online risks (e.g. AI misuse, deepfakes, scams, harmful trends).
- Lessons learned from incidents will directly inform curriculum updates, staff training priorities, and technical safeguards.
- Where gaps are identified, targeted action will be taken to strengthen the school's e-safety approach.

Appencies

Appendix A - Student E-Safety Agreements

My Oasis Therapeutic Alternative Provision

Student Agreements

My Oasis Student Behaviour and Personal Electronic Device Contract

Student Name: _____Date:_____

Purpose of this Contract

At My Oasis, we believe that every student deserves a safe, respectful, and positive learning environment. This contract explains the rules, expectations, and support available to help you succeed at school.

Our Approach to Behaviour

- At My Oasis, we understand that behaviour is often a way of communicating.
  We aim to support students in understanding and managing their behaviour using a holistic, nurturing, and trauma-informed approach.
- Consequences are decided taking into account all circumstances.
- Staff work with students to help them learn from their choices and develop positive strategies.
- Support is available at all times.
- Our goal is to create a place where students feel safe, understood, and empowered, rather than simply punished.

School Expectations

1. Respect Others

- Treat staff, students, and visitors with kindness and fairness.
- Do not bully, harass, or discriminate against anyone.
- Help others feel safe and included.

2. Follow Instructions

- Listen and follow staff instructions the first time they are given.
- Staff are here to keep you safe and help you succeed.

3. Be Prepared to Learn

- Arrive at school and lessons on time and ready to learn.
- Bring all materials needed and complete your work.
- Take part in lessons and activities positively.

4. Behave Responsibly

- Stay focused on learning and avoid disrupting others.
- Keep your hands, feet, and objects to yourself.
- Use polite and appropriate language.
- Do not engage in physical or verbal aggression, intimidation, or violence.
- Understand that your behaviour affects other students' right to learn.

5. Take Care of the School Environment

- Keep classrooms and school areas clean and tidy.
- Respect school property and the belongings of others.
- Report any damage or safety concerns to staff.

Personal Electronic Device Policy

- Personal devices (phones, tablets, laptops) must not be brought to school unless approved by school leadership.
- If brought without permission, devices will be stored safely and returned at the end of the day.
- My Oasis is not responsible for any loss, damage, or theft of personal devices.
- Repeated breaches may lead to further consequences or parent/carer meetings.

Prohibited Items (Contraband)

Do not bring any items that are illegal, dangerous, or inappropriate.

A. Electronic Devices

- Phones, tablets, laptops, or other electronic devices without permission.
- Devices that can record or access the internet unsupervised.

B. Smoking & Vaping

- Cigarettes, vapes, e-cigarettes, lighters, matches, or related items.

C. Drugs, Alcohol, and Intoxicating Substances

- Illegal drugs, alcohol, and drug-related items.
- Energy drinks, aerosols, or substances for misuse.

D. Weapons & Dangerous Objects

- Knives, firearms, imitation weapons, fireworks, explosives.

E. Stolen or Offensive Materials

- Stolen goods, offensive or discriminatory materials, pornographic or violent items.

F. Money, Medication, or Restricted Items

- Cash or valuables unless signed in by parent/carer.
- Medication, unless signed in by parent/carer.
- Any item that staff consider unsafe or disruptive.

This list is not exhaustive. Staff can confiscate and/or store any unsafe, inappropriate, or disruptive items.

Consequences

If you do not follow this contract, consequences may include:

- Verbal warning

- Detention
- Time-out or reflection
- Restorative conversation
- Parent/carer meeting
- Meetings with external professionals (e.g., police, youth workers, or other relevant agencies) to discuss behaviour, safety, or related issues
- Suspension or exclusion in serious or repeated cases

Support and Guidance

- My Oasis will help you make positive choices:
- Mentoring
- Counselling
- Behaviour support plans
- Pastoral care or wellbeing interventions
- Support from external professionals (e.g., police, youth workers, or relevant agencies) as needed
- Family or external agency support

Policy References

Please refer to the following My Oasis policies:

- E-Safety Policy
- Mobile Phone Policy
- Behaviour Policy
- Suspensions and Exclusions Policy
- Safeguarding Policies

Accessibility Support

- This contract can be read aloud to students who need support.
- Photos, icons, or visual aids are available to help explain the rules.
- Translated versions, Contracts on Coloured Paper and overlays are available on request for students or parents/carers.
- Staff can explain any part of the contract to ensure everyone understands it.

Agreement

Student Signature: _____

I understand and agree to follow the expectations set out in this contract.

Parent/Carer Signature: _____

I have read and discussed this contract with my child and support the school's expectations.

Staff Member Signature: _____

I have explained this contract to the student and will support them in meeting these expectations.

Record Keeping

A signed copy of this contract will be kept in your personal school file, and a copy will be provided to you and your parent/carer for your records.

My Oasis School Device Acceptable Use Contract

Student Name: _____ Date: _____

Purpose of this Contract

At My Oasis, school devices such as laptops, tablets, and computers are provided to help you learn, communicate, and explore safely.

This contract explains how to use school devices responsibly, safely, and respectfully.

Our Approach

- We understand mistakes happen, and learning safe technology use is part of growing up.
- Staff use a trauma-informed, nurturing, and holistic approach to support students.
- Consequences are decided based on the full context of each situation.
- Support is available at all times for using devices safely and responsibly.

---

1. General Rules for School Devices

- School devices are for learning and school-related activities only.
- Handle devices carefully and return them in good condition.
- Keep your login, passwords, and personal information private.
- Work with supervising staff: you must allow staff to see your screen at all times to ensure safe and responsible use.
- Report anything unsafe, concerning, or broken immediately to a staff member.

---

2. Respectful Use

- Use polite and appropriate language when online or using apps.
- Do not bully, harass, or threaten anyone using school devices.
- Respect other people's work, privacy, and files.
- Do not share personal information about yourself or others.

---

3. Internet and Applications

- Only access websites, programs, or apps approved by staff.
- Do not download or install software without permission.
- Avoid clicking on unknown links or attachments.
- Remember that staff will monitor device use to keep you safe.

---

4. Device Security

- Do not attempt to bypass passwords, firewalls, or security settings.
- Keep your device safe and do not leave it unattended.
- Report lost, stolen, or damaged devices immediately.

---

5. Consequences

If you do not follow this contract, consequences may include:

- Verbal warning
- Detention
- Time-out or reflection period

- Parent/carer meeting
- Meetings with external professionals (e.g., police, youth workers, or other relevant agencies) if online behaviour is unsafe or illegal
- Suspension or exclusion in serious or repeated cases

Staff will always consider the circumstances and use a holistic, trauma-informed approach.

---

6. Support and Guidance

- Staff will provide guidance on safe and responsible use of school devices.
- Mentoring or counselling support is available if issues arise.
- Family or external agency support may be offered for ongoing concerns.

---

7. Accessibility Support

- This contract can be read aloud to students who need help.
- Visual aids or icons are available to help explain the rules.
- Translated versions, Contracts on Coloured Paper and Overlays are available upon request for parents/carers or students.
- Staff are available to answer questions to ensure full understanding.

---

8. Policy References

Please also refer to My Oasis policies:

- E-Safety Policy
- Behaviour Policy
- Safeguarding Policies

---

9. Use of AI Tools

- AI tools (e.g., ChatGPT, Bing AI, or other generative AI programs) must only be used for learning and school-related purposes.
- You must not use AI to cheat, plagiarise, or bypass your own learning; all work submitted must reflect your own understanding.
- Follow staff instructions when using AI tools. Staff will ask to see your screen or review AI-generated content.
- Do not use AI to create harmful, offensive, or inappropriate content.
- Report any AI content that is unsafe, inaccurate, or concerning to a staff member immediately.
- Misuse of AI tools may result in the same consequences as other unacceptable device use, including detention, parent/carer meetings, or loss of device access.

---

10. Agreement

Student Signature: _____

I understand and agree to use school devices safely, responsibly, and respectfully.

Parent/Carer Signature: _____

I have read and discussed this contract with my child and support the school's expectations.

Staff Member Signature: _____

I have explained this contract to the student and will support them in using school devices safely.

Record Keeping

A signed copy of this contract will be kept in your personal school file and a copy will be provided to you and your parent/carer.

Please note that staff agreements are also completed during induction.