Olive Academies Independent School

OA-North View

ICT & Online Safety Policy

Document control table	
Title	ICT & Online Safety Policy
Date updated and approved	August 2026
Approved by	OAISB
Date of next review	August 2027
Updates/revisions included:	Added in the additional responsibilities of the Board to review filtering and monitoring and the need to consider risk of AI. Updated in line with KCSIE 2026 ensuring safeguarding concerns are recorded as current or historic. Leaders must ensure cyber risk assessments are conducted annually and cyber awareness plan is implemented. Explicit online safety and the risks of AI will be taught to pupils.
This policy applies to Olive Academies Independent School OA-North View and should be implemented consistently throughout the school. Proposed amendments should be referred to the Head of School/Executive Headteacher and OAISB for consideration **Please note the acceptable use agreements are to be completed by all pupils and their parents/carers – sample of these are in Appendix 3. Staff complete acceptable use agreements as part of their Staff Declaration.**	

This policy forms part of the school's wider safeguarding framework. Online safety is recognised as a safeguarding issue and all concerns will be managed in accordance with the Child Protection and Safeguarding Policy. The school will take all reasonable steps to protect pupils from harm when using technology and online services.
The school recognises that online safety is fundamental to promoting pupils' welfare and fulfilling its duties under Part 3 of the Independent School Standards.

Contents

1 Introduction and overview 4
2 The 4 key categories of risk 4
3 Scope 5
4 Legislation and guidance 5
5 Roles and responsibilities 6
6 Communication 10
7 Educating pupils about online safety 11
7.1 Pupil online safety curriculum 11
8 Training and awareness raising 12
9 Accessibility 14
10 Child-on child sexual abuse and harassment 14
11 Handling online safety and cyber-bullying concerns and incidents 15
12 Cyberbullying 16
13 Misuse of technology – (devices, systems, networks or platforms) 16
14 Social media incidents 16
15 Use of equipment and digital content 17
15.1 Personal mobile devices (mobile phones, tablets and other mobile devices) 17
15.2 Pupils' use of personal devices 17
15.3 Staff use of personal devices 18
15.4 Digital images and video 18
16 Artificial Intelligence (AI) 19
17 Examining electronic devices 19
18 Managing the IT infrastructure 21
18.1 Internet access, security (virus protection) filtering and monitoring 21
18.2 Network management (user access, backup) 21
19 Password policy 23
20 Email 23
21 School website 24

22 Cloud environments 24
23 CCTV 24
24 Data security: Management Information System access and data transfer 24
24.1 Strategic and operational practices 25
24.2 Technical solutions 25
25 Reviewing and monitoring this policy 25
26 Appendix 1 – Good practice guidance on the use of images 26
26.1 Photographs taken by parents at School events 27
27 Appendix 2: Online safety training needs – self-audit for staff 28
28 Appendix 3: Acceptable use agreements for parents and carers 28
29 Appendix 4: Acceptable use agreement for older pupils 29
30 Appendix 5: Acceptable use agreement for younger pupils 30

1 Introduction and overview

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of this School with respect to the use of IT-based technologies
- Facilitate the safe, responsible and respectful use of technology to support teaching and learning, increase attainment and prepare children and young people for the risks and opportunities of the digital world, to survive and thrive online
- Safeguard and protect children and staff
- Assist staff working with children to work safely and responsibly with the internet and other IT and communication technologies and to monitor their own standards and practice
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use for the whole School community
- Have clear structures to deal with online abuse such as online bullying [noting that these need to be cross referenced with other School policies]
- Ensure that all members of the School are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

2 The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism

Contact – being subjected to harmful online interaction with other users, such as 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, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

3 Scope

This policy applies to all members of this School (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of the School IT systems, both in and out of the School.

4 Legislation and guidance

This policy sits within, and complies with, the following legislation and guidance:

- Keeping Children Safe in Education
- Data Protection Act 2018
- The General Data Protection Regulation
- Computer Misuse Act 1990
- Human Rights Act 1998
- Equality Act 2010
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- The Education and Inspections Act 2006
- Searching, screening and confiscation: advice for schools
- Harmful online challenges and online hoaxes (DfE 2021)
- Department for Science, Innovation and Technology and UK Council for Internet Safety (2024) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'

This policy also takes into account the Department for Education's advice for schools on:

- Teaching online safety in school
- Education for a Connected World
- Relationships and sex education
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Searching, screening and confiscation
- and guidance on protecting children from radicalisation.
- Filtering monitoring standards (DfE 2024)

Within existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyberbullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so. It also reflects the emphasis made in Keeping Children

Safe in Education (KCSIE) which has changed to give online safety the prominence it deserves in the main body of the guidance – making clear that the management of online safety is a key part of ensuring a thorough safeguarding approach across the School and the trust.

This policy supports compliance with:

- Independent School Standards Part 2 (Spiritual, Moral, Social and Cultural Development of Pupils)
- Independent School Standards Part 3 (Welfare, Health and Safety of Pupils)
- Independent School Standards Part 5 (Premises and Accommodation with regard to CCTV and security arrangements)
- Independent School Standards Part 8 (Quality of Leadership and Management)

The Proprietor Body ensures that effective arrangements are in place to safeguard and promote the welfare of pupils through the safe and responsible use of technology.

It should be read in conjunction with other OA-North View policies including:

- Safeguarding and child protection
- Anti-bullying
- Behaviour and Relationships Policy
- Relationships, sex education and Health Policy
- PSHE
- Data protection
- Staff code of conduct
- Social Media Policy
- Searching, screening and confiscation policy

These policies are available either on the website or via the staff intranet

5 Roles and responsibilities

Role	Key responsibilities
The Proprietor Body, Olive Academies Independent School Board (OAISB), has	The OAISB will undertake an annual review of filtering and monitoring arrangements and receive regular reports from the Head of School/Designated Safeguarding Lead regarding online safety incidents, trends, training and safeguarding concerns. The OAISB will seek assurance that:

Role	Key responsibilities
overall responsibility for ensuring compliance with the Independent School Standards, safeguarding requirements and online safety arrangements	• Appropriate filtering and monitoring systems are effective; • Staff receive suitable online safety training; • Pupils receive an age-appropriate online safety curriculum; • Safeguarding concerns relating to online activity are identified and managed appropriately; and • The school meets its responsibilities under KCSIE and the Independent School Standards.
OA Trust Safeguarding Lead	Responsible for ensuring there is a consistent approach taken to online safety across the schools within Olive Academies and that practice and incidents are logged and reviewed on a regular basis.
Head of School (or equivalent)	Responsible for: • ensuring that staff understand this policy and that it is being implemented consistently though the school. • Supporting the DSL and the deputy DSL by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
Designated Safeguarding Lead	**The DSL takes lead responsibility for online safety in the School, in particular:** • Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school • Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents • Managing all online safety issues and incidents in line with the school child protection policy • Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy • Ensuring that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life. • Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy

Role	Key responsibilities
	The Headteacher and DSL will undertake an annual online safety risk assessment which will consider: • local safeguarding trends; • emerging technologies; • risks associated with artificial intelligence; • pupil vulnerabilities; • filtering and monitoring effectiveness; • cyber security threats. • Updating and delivering staff training on online safety (section 8 provides a summary of our approach and appendix 4 contains a self-audit for staff on online safety training needs) • Liaising with other agencies and/or external services if necessary • Providing regular reports on online safety in school to the headteacher and lead trustee and AAB member for safeguarding • Maintaining detailed, secure and accurate written records of reported online safety concerns and the decisions and whether referrals have been made. • Understanding the purpose of record keeping • Understanding the filtering and monitoring processes in place at the School. • Ensuring records of filtering and monitoring reviews are maintained, and that any safeguarding concerns are clearly recorded as current or historic, in line with KCSIE 2026." "The DSL will ensure that online safety training and updates for staff include content on generative AI, deepfakes, misogynistic influencers, and the links between online safety and mental health. This list is not intended to be exhaustive.
Trust Facilities & Infrastructure Manager	• Ensuring there are in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils

Role	Key responsibilities
	are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material • Ensuring that the trust's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly • Conducting a full security check and monitoring the trust's ICT systems monthly • Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files This list is not intended to be exhaustive.
Computing Curriculum lead (generally the QE lead)	• As listed in the 'all staff' section plus: • To oversee the delivery of the online safety element of the computing curriculum • Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within computing • Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable use agreements See appendix 3 The IT lead will ensure that cyber risk assessments are conducted annually, and that a cyber awareness plan is implemented for staff and pupils.
Data Protection Officer (refer to data protection policy for more detail)	• To ensure that the data they manage is accurate and up-to-date and in line with GDPR legislation. • Ensure best practice in information management. i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements. • Ensure personal data breaches are reviewed and reported to the ICO as relevant • The School must be registered with Information Commissioner by OA central.
All staff	All staff, including contractors and agency staff, and volunteers are responsible for: • Maintaining an understanding of this policy • Implementing this policy consistently and participating in trust training • Agreeing and adhering to the terms on acceptable use of the trust's ICT systems and the internet and ensuring that pupils follow the trust's terms on acceptable use

Role	Key responsibilities
	• Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy • Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy • Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here' This list is not intended to be exhaustive. **Exit strategy (where relevant)** At the end of the period of employment to return any equipment or devices loaned by the School. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to log in and allow a factory reset.
Parents/carers	• Ensure their child has read, understood and agreed to the terms on acceptable use of the School's ICT systems and internet • To consult with the School if they have any concerns about their children's use of technology. • To support the School in promoting online safety and endorse the pupil's acceptable use agreement which includes the pupils' use of the internet and the School's use of photographic and video images – this is included in the parental permissions and should be shared with parents on induction.
Visitors and members of the community	• Visitors and members of the community who use the School's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use and should they wish to use the wi-fi within a setting, they will need to accept the terms and conditions and abide by these.

6 Communication

The policy will be communicated to staff, pupils and their parents/carers in the following ways:

- policy to be posted on the School website
- policy to be part of School induction pack for new staff
- regular updates and training on online safety for all staff
- acceptable use agreements (within staff declaration) discussed with staff at the start of each year and confirms staff have read and understood this policy

- acceptable use agreements to be issued to pupils and parents on admission or at the start of the year depending on when the pupil is placed in the School (see appendix 3).

7 Educating pupils about online safety

7.1 Pupil online safety curriculum

Pupils will be taught about online safety as part of the curriculum: We also follow the guidance on relationships education, relationships and sex education (RSE) and health education.

All schools must teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

Online safety education will include explicit teaching about the risks of generative AI, deepfakes, online misogyny, and the influence of online personalities. The curriculum will also address the links between online activity and mental health, and staff will be trained to spot and respond to warning signs.

At OA-North View, staff recognise that pupils with social, emotional and mental health needs may be particularly vulnerable to online exploitation, grooming, harmful online communities, radicalisation, self-harm content, misogynistic influencers, criminal exploitation and coercion. Online safety education is therefore adapted to individual need and delivered through a trauma-informed approach. Staff will provide additional support where required to help pupils understand risks, regulate online behaviours and develop safe digital habits.

In **Key Stage 3**, pupils will be taught to:

- understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- recognise inappropriate content, contact and conduct, and know how to report concerns.

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

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

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

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online

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

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

The School will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

Online safety education contributes to pupils' spiritual, moral, social and cultural development by helping them:

- understand right and wrong online;
- respect the views and rights of others;
- recognise and challenge discrimination, bullying and extremist views;
- develop resilience, responsibility and positive relationships;
- prepare for life in modern Britain.

Through online safety education, pupils are also supported to understand fundamental British values, including mutual respect, individual liberty and tolerance of those with different faiths and beliefs, and to recognise and challenge extremist, discriminatory or unlawful online content.

8 Training and awareness raising

All new staff members will receive training, as part of their induction, on safe internet use, cyber security awareness and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse other children **online through:**
- Abusive, harassing, and misogynistic messages
- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to **ensure pupils can recognise dangers and risks in online activity and can weigh up the risks**
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills about online safety at regular intervals, and at least annually.

Trustees and AAB members will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

When recording safeguarding concerns, staff must clearly distinguish between current and historic concerns, in line with KCSIE 2026

Parent awareness and training

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents via the website.

Online safety will also be covered during parents' evenings.

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

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

- What are the issues? UK Safer Internet Centre: www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: www.childnet.com/parents-and-carers/hot-topics

9 Accessibility

The School will ensure that digital accessibility is considered in all relevant strategies and communications, so that all pupils, staff, and parents can access information and systems

10 Child-on child sexual abuse and harassment

All staff will be aware of the indicators of abuse, neglect and exploitation and understand where the risk of such harms can occur online. Staff will understand that this can occur both in and outside of the School, off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery
- Abuse between young people in intimate relationships online, i.e. teenage relationship abuse

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a culture that normalises abuse and leads to pupils becoming less likely to report such conduct.

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

The School will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other pupils taking "sides", often leading to repeat harassment. The School will respond to these incidents in line with the **Child-on-child Abuse Policy** and the **social media policy**.

The School will respond to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the School premises or using School-owned equipment. Concerns regarding online child-on-child abuse will be reported to the DSL, who will investigate the matter in line with the **Child-on-child Abuse Policy** and the **Child Protection and Safeguarding Policy**.

Where online behaviour occurring outside school is likely to have an impact on the welfare, safety or education of pupils within school, the school will take appropriate action in accordance with the Behaviour Policy, Child Protection and Safeguarding Policy and relevant statutory guidance.

11 Handling online safety and cyber-bullying concerns and incidents

OA-North View recognises that online incidents may be linked to wider safeguarding concerns including child-on-child abuse, criminal exploitation, county lines activity, mental health concerns, attendance difficulties and harmful peer relationships. Online safety concerns will therefore always be considered within the wider context of the pupil's lived experience and safeguarding history.

General concerns must be handled in the same way as any other safeguarding concern; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should always talk to the designated safeguarding lead as information contributes to the overall picture or highlight what might not yet be a problem.

Non-teaching staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence).

OA commits to take all reasonable precautions to ensure online safety but recognises that incidents will occur both inside and outside the School (and that those from outside the School will continue to impact on pupils when they come into the School). All members of the School are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the School's escalation processes.

Any suspected online risk or infringement should be reported to the designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson.

Any concern/allegation about staff misuse is always referred directly to the headteacher or executive headteacher, Any safeguarding allegation concerning the Headteacher will be referred to the Chair of the OAISB and managed in accordance with the Child Protection and Safeguarding Policy and statutory guidance.

Staff may also use the NSPCC Whistleblowing Helpline 0800 028 0285, help@nspcc.org.uk

OA will actively seek support from other agencies as needed (e.g. the local authority, UK Safer Internet Centre's Professionals' Online Safety Helpline, NCA CEOP, Prevent Officer, Police, IWF). We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law (procedures are in place for sexting; see section below)

12 Cyberbullying

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

Cyberbullying should be treated like any other form of bullying and the school anti-bullying policy should be followed for cyber-bullying, which may also be referred to as cyberbullying. OA's anti-bullying policy provides detail on how the School treats bullying and procedures in place to support pupils who are bullied and who bully.

In addition, the School will implement a cyber awareness plan for pupils and staff to ensure that they understand the basics of cyber security and protecting themselves from cyber crime.

The School will implement it's cyber security strategy in line with the DfE's 'Cyber security standards for schools and colleges'.

Materials to support teaching about bullying and useful Department for Education guidance and case studies are at bullying.lgfl.net

The School will conduct an annual cyber risk assessment and implement a cyber awareness plan for pupils and staff. Digital technology will be included in the school's disaster recovery and business continuity plans.

13 Misuse of technology – (devices, systems, networks or platforms)

Where a pupil misuses the School's ICT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the School's ICT system or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The School will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

14 Social media incidents

See the social media section later in this document for rules and expectations of behaviour for children and adults in our School. These are also governed by the trust's acceptable use policies and staff social media policy.

Breaches will be dealt with in line with the School behaviour policy (for pupils) or code of conduct (for staff).

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the School community, OA will request that the post be deleted and will expect this to be actioned promptly.

Where an offending post has been made by a third party, the School may report it to the platform it is hosted on and may contact the Professionals' Online Safety Helpline (run by the UK Safer Internet Centre) for support or help to accelerate this process.

15 Use of equipment and digital content

15.1 Personal mobile devices (mobile phones, tablets and other mobile devices)

- Mobile devices brought into the School are entirely at the staff member, pupils & parents or visitors' own risk. The School accepts no responsibility for the loss, theft or damage of any phone or handheld device brought into School.
- Mobile devices are not permitted to be used in certain areas within the School site, e.g. pupil changing rooms and toilets.
    - No images or videos should be taken on mobile devices without the prior consent of the person or people concerned.
    - The Bluetooth or similar function of a mobile device should not be used to send images or files to other mobile devices.
    - All visitors are requested to keep their phones unseen and on silent.
    - All mobile device use is to be open to monitoring scrutiny and the headteacher is able to withdraw or restrict authorisation for use at any time, if it is deemed necessary.
- In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the School reserves the right to search the content of any mobile devices on the School premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying.

15.2 Pupils' use of personal devices

- In line with statutory guidance from September 2026, pupils must not have access to their mobile phones at any time during the school day.
    - Smart Watches should not be worn and will be confiscated until the end of the day if a pupil is found to be wearing one
- Should pupils be found with a mobile device during the day, the device will be confiscated in line with the School's behaviour policy. We reserve the right to use search devices such as security wands to identify pupils carrying mobile phones in contradiction with the acceptable use agreement.
- If a pupil needs to contact their parents or carers, they will be allowed to use an School phone or in exceptional circumstances, their own phone under supervision. Parents are advised not to contact their child via their mobile phone during the School day, but to contact the School office.

- Pupils are not permitted to use personal mobile phones or devices as part of an educational activity.

15.3 Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices in a professional capacity, such as for contacting children, young people or their families within or outside of the setting. There may be exceptional circumstances where members of the Senior Leadership Team need to use their own mobile phones in the absence of the availability of an School phone or landline.
- Staff will be issued with an School phone where contact with pupils, parents or carers is required, for instance for off-site activities.
  - Personal mobile phones or devices will be switched off or switched to 'silent' mode. They will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
  - Staff should not use personal devices to take photos or videos of pupils and will only use work-provided equipment for this purpose.
  - Staff may use their phones during break times and other non-contact time in designated staff rooms or an office where pupils are not present.
- In an emergency where a staff member doesn't have access to an School-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes and then report the incident with the headteacher / designated officer.
  - Staff should also refer to the OA social media policy which provides guidelines on use of personal and professional use of social media.
- If a member of staff breaches the School policy, then disciplinary action may be taken.
  - If there is a safeguarding concern about the content of a member of staff's mobile phone, the headteacher reserves the right to search the phone or contact the police.

15.4 Digital images and video

In this School:

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the School agreement form when their child joins the School.
  - We do not use first names to identify pupils in pictures online, in print or in videos unless there is a specific need, e.g. celebrating a success – in which case individual consent will be obtained. We do not use full names.
- If specific pupil photos (not group photos) are used on the School website, in the prospectus or in other high-profile publications the School will obtain individual parental or pupil permission for its long-term, high-profile use;
- Staff sign the School's Acceptable Use Policy within the annual staff declaration, and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils;

- Pupils are taught about how images can be manipulated in their online safety education programme and taught to consider how to publish for a wide range of audiences which might include trustees, AAB members, parents or younger children as part of their computing scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Further guidance on the use of images is available in Appendix 1

16 Artificial Intelligence (AI)

In this School we recognise that:

- Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.
- That AI has many uses to help pupils learn but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

OA-North View will treat any use of AI to bully pupils in line with our anti-bullying policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

Staff must not input confidential, personal or safeguarding information relating to pupils into public AI platforms unless approved systems with appropriate data protection safeguards are being used.

17 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Assess how urgent the search is and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the DSL
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason'.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL and headteacher (advised by the Trust Safeguarding Lead) to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

18 Managing the IT infrastructure

18.1 Internet access, security (virus protection) filtering and monitoring

Filtering and monitoring systems will be reviewed at least once every academic year, and these reviews will specifically consider new and emerging risks, including those posed by generative AI (e.g. deepfakes, AI-generated content). Reviews will be led by the senior leader responsible for filtering and monitoring, with support from the DSL and IT support, and records will be kept of all reviews and actions taken.

Records of filtering and monitoring reviews will be retained and made available to the Board for scrutiny.

School will:

- inform all users that Internet/email use is monitored
- have the educational filtered secure broadband connectivity through Schools Broadband
- use the Senso filtering system which blocks sites that fall into categories (e.g. adult content, race hate, gaming). All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status
- use USO user-level filtering where relevant
- ensure network health through use of Sophos anti-virus/anti-malware software
- use Microsoft office encrypted email service to send 'protect-level' (sensitive personal) data over the Internet
- use encrypted devices or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site
- work in partnership with the external IT provider to ensure any concerns about the system are communicated so that systems remain robust and protect pupils.

The Executive Headteacher is the senior leader with day-to-day responsibility for filtering and monitoring. The DSL will take lead responsibility for safeguarding responses arising from filtering and monitoring systems. The Proprietor Body will receive regular assurance that filtering and monitoring arrangements remain effective and appropriate to identified risks.

18.2 Network management (user access, backup)

Academies:

- use individual, audited logins for all users

- use guest accounts occasionally for external or short-term visitors for temporary access to appropriate services
- use teacher 'remote' management control tools for controlling workstations/viewing users/setting-up applications and Internet web sites, where useful
- require the technical support provider to be up to date with local authority services and policies
- have daily back-up of School data (admin and curriculum)
- use secure, 'Cloud' storage for data back-up that conforms to DfE guidance
- storage of all data within the School will conform to the UK data protection requirements
- storage of data online, will conform to the UK data protection EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, academies:

- ensure staff read and sign that they have understood the School's online safety policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. OA also provide a different/use the same username and password for access to the OA network across academies.
- ensure all pupils can access their individual accounts and store all work onto the pupil area
- make clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins
- have set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas
- require all users to log off when they have finished working or are leaving the computer unattended
- ensure all equipment owned by the School and/or connected to the network has up to date virus protection
- make clear that staff are responsible for ensuring that any computer or laptop loaned to them by the School, is used to support their professional responsibilities
- maintain equipment to ensure health and safety is followed
- ensure that access to the School's network resources from remote locations by staff is audited and restricted and access is only through School approved systems
- do not allow any outside agencies to access our network remotely except where there is a clear professional need and then access is audited restricted and is only through approved systems
- have a clear disaster recovery system in place that includes a secure, remote off site back up of data
- use secure data transfer; this includes DfE secure S2S website for all CTF files sent to other schools
- ensure that all pupil level data or personal data sent over the Internet is encrypted and only sent through ARBOR or encrypted email

- wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use
- IT and communications systems are installed professionally and regularly reviewed to ensure they meet health and safety standards.

19 Password policy

- This School makes it clear that staff and pupils must always keep their passwords private, must not share with others; If a password is compromised the School should be notified immediately.
- All staff have their own unique username and private passwords to access School systems. Staff are responsible for keeping their password(s) private.
- We require staff to use STRONG passwords.
- We require staff using critical systems to use two factor authentication.

20 Email

Academies:

- provide staff with an email account for their professional use and makes clear personal email should be through a separate account
- will contact the police if one of our staff or pupils receives an email that we consider is particularly disturbing or breaks the law.
- will ensure that email accounts are maintained and up to date
- use a number of technologies to help protect users and systems in the School, including desktop anti-virus and anti-malware product Sophos, plus direct email filtering for viruses.

Pupils:

- To ensure OA has in place an effective remote learning programme (see below), pupils will have access to an OA email account.
- These email accounts will be intentionally 'anonymised' for pupil protection and will be restricted to internal mails within the OA network.
- Pupils are taught about the online safety and 'etiquette' of using email both in the School and at home.

Staff:

- Staff can only use the Olive Academies email systems on the School system
- Staff will use OA email systems for professional purposes

- Access in the School to external personal email accounts may be blocked
- **Send staff/pupil data by secure file transfer and minimise use of encrypted email.**

21 School website

- The headteacher, supported by OA central, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained
- The web site should comply with statutory DFE requirements and this will be monitored by OA central
- Most material is the School's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status
- Photographs published on the web do not have names attached – if a photo of an individual child is used, their first name is not included. In rare cases where this might be considered important, e.g. a case study of successful outcomes, specific parent/carer permission would be needed. We do not use pupils' names when saving images in the file names or in the tags when publishing to the School website.

Further guidance on the use of images is available in Appendix 1

22 Cloud environments

- Uploading of information on the School's online learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas
- Photographs and videos uploaded to the School's online environment will only be accessible by members of the School community
- In the School, pupils are only able to upload and publish within School approved 'Cloud' systems.

23 CCTV

- We have CCTV academies as part of our site surveillance for staff and pupil safety. The use of CCTV is clearly signposted in each School. We will not reveal any recordings without appropriate permission. Our CCTV systems policy is available on our website.
- We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.

24 Data security: Management Information System access and data transfer

24.1 Strategic and operational practices

Academies:

- The headteacher works with the OA data protection officer to ensure a GDPR compliant framework for storing data but which ensures that child protection is always put first and data protection processes support careful and legal sharing of information
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in a single central record

24.2 Technical solutions

- Staff have secure area(s) on the network to store sensitive files.
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 10 minutes idle time.
- All servers are cloud based or in lockable locations and managed by DBS-checked staff.
- Details of all School-owned hardware will be recorded in a hardware inventory.
- Details of all School-owned software will be recorded in a software inventory.
- Disposal of any equipment will conform to the Waste Electrical and Electronic Regulations. Further information can be found here - https://www.gov.uk/electricalwaste-producer-supplier-responsibilities and on the Environment Agency website.
- Where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data.
- We are using secure file deletion software.

25 Reviewing and monitoring this policy

The online safety policy will be reviewed annually and additionally following:

- significant changes to statutory guidance;
- safeguarding incidents indicating the need for review;
- changes to filtering or monitoring systems;
- significant developments in technology, including artificial intelligence;
- recommendations arising from audits, inspections or safeguarding reviews.

26 Appendix 1 – Good practice guidance on the use of images

This guidance covers the use of images on:

- School websites
- Social Media channels (Twitter, LinkedIn, Facebook etc.)
- School brochures, newsletters and press releases

'Images' and 'photographs' also cover video recordings.

Permissions

- Before taking/using images of pupils always check that parental permission has been granted in the parental consent form of the Pupil Induction Pack.
- Always check verbally with pupils as well and make sure that pupils are clear on how the photo will be used and what it is illustrating.
- Remember you'll also need to get consent from any teachers that are photographed
- Additional consent may be needed for specific cases of photography, filming that are being used for wider publicity, e.g. a film about the trust, or a brochure with a case study about a child.

Use of names

- If a child's image is used do not use their name to accompany the image.
- If a child is named do not use an accompanying photograph.
- A rare exception to naming a child would be, for example, a case study about a child's progress, in which case specific parental/pupil consent would need to be obtained

Further guidelines

- Only use images of children in suitable clothing to reduce the risk of inappropriate use. Some activities, for example swimming and drama, present a much greater risk of potential misuse.
- Pupils must be wearing correct uniform (unless taking part in an outdoor activity or special event)
- When possible, show groups of pupils doing activities together without faces being shown.
- Focus on showing pupils in groups rather than individual close-ups – use captions such as "An English lesson/Science experiment" or "Making Christmas decorations".
- Make sure that any visiting press photographers are made aware of OA guidelines on the use of images/names.
- Don't use images that could cause distress, upset or embarrassment to pupils or their families.
- If using an individual pupils' image on website/brochure, specific individual parental/pupil permission should be sought for high-profile use.
- Reflect different ethnic backgrounds and diversity.
- Images of pupils and teachers who have left the School should be promptly removed from the website.

Dealing with media/Press

- Let pupils and parents know that a journalist/ photographer will be in attendance at an event and ensure parents have signed the parental consent form of the Pupil Induction Pack.
- Do not allow photographers unsupervised access to pupils.
- Issue the photographer with ID that must be always worn.
- Provide a clear brief to professional photographers/press regarding Olive Academies' expectations of them in relation to child protection and safeguarding.
- Ask the journalist/ photographer to use a group shot, not an individual photograph.

Please contact OA's Communications and Marketing Manager, Charlotte Crooks for advice and guidance prior to working with media/press.

26.1 Photographs taken by parents at School events

The School should inform parents before events that any images taken during events are for personal and domestic use and no other use. They should not be shared on social media.

Use of equipment

Images should only be taken and stored on School equipment, which should not leave the School.

Storing of images

Images or recordings should be securely stored. Hard copies of images should be kept in a locked drawer and electronic images should be in a protected folder with restricted access.

Images should not be stored on unencrypted portable equipment such as laptops, memory sticks and mobile phones. Image filenames should not use pupils' names. Images of pupils or teachers who have left the School should be destroyed/deleted.

Organisations who are storing and using photographs to identify children and adults for official purposes, such as identity cards, should ensure they are complying with the legal requirements for handling personal information. Further guidance on the Data Protection Act and other privacy regulations can be found on the Information commissioner's office website.

Further guidance regarding photographing and recording children during events and activities can be found on the NSPCC website

27 Appendix 2: Online safety training needs – self-audit for staff

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
Do you know the name of the person who has lead responsibility for online safety in the School?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the School's acceptable use agreement for staff (contained within the annual staff declaration)?	
Are you familiar with the School's acceptable use agreement for pupils and parents (contained within the home School agreement?	
Do you regularly change your password for accessing the School's ICT systems?	
Are you familiar with the School's approach to tackling cyber-bullying?	
Have you read and understood the OA social media policy?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	

28 Appendix 3: Acceptable use agreements for parents and carers

Acceptable use of the internet: agreement for parents and carers

Name of parent/carer: **Name of child:**
Online channels are an important way for parents/carers to communicate with, or about, our school. The School uses the following channels: • email/text groups for parents (for school announcements and information) • our virtual learning platform Microsoft Teams Staff also set up independent channels for Parents/carers to help them stay on top of what is happening in their child's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp).
When communicating with the school via official communication channels, or using private/independent channels to talk about the school, **I will:** • be respectful towards members of staff, and the school, at all times • be respectful of other parents/carers and children • direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure **I will not:** • use private groups, or personal social media to complain about or criticise members of staff. This is not constructive and the school cannot improve or address issues if they are not raised in an appropriate way • use private groups, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident • upload or share photos or videos on social media of any child other than my own, unless I have the permission of other children's parents/carers

Signed:	**Date:**

29 Appendix 4: Acceptable use agreement for older pupils

Acceptable use of the School's ICT facilities and internet: agreement for pupils and parents/carers
Name of pupil:

When using the School's ICT facilities and accessing the internet in school,

I will not:

- use them for a non-educational purpose
- use them without a teacher being present, or without a teacher's permission
- use them to break school rules
- access any inappropriate websites
- access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
- use chat rooms
- open any attachments in emails, or follow any links in emails, without first checking with a teacher
- use any inappropriate language when communicating online, including in emails
- share my password with others or log in to the school's network using someone else's details
- bully other people
- Use generative AI tools to create or share harmful, inappropriate, or misleading content (e.g. deepfakes or AI-generated images/videos of others)

Also:

- I understand that the school will monitor the websites I visit and my use of the School's ICT facilities and systems.
- I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.
- I will always use the School's ICT systems and internet responsibly.
- I understand that the School can discipline me if I do certain unacceptable things online, even if I am not in school when I do them.

Signed (pupil):	Date:

- **Parent/carer agreement:** I agree that my child can use the School's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the School's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	Date:

30 Appendix 5: Acceptable use agreement for younger pupils

Acceptable use of the School's ICT facilities and internet: agreement for pupils and parents/carers
Name of pupil:
When I use the School's ICT facilities (like computers and equipment) and get on the internet in school,

I will not:

- use them without asking a teacher first, or without a teacher in the room with me
- use them to break school rules
- go on any inappropriate websites
- go on Facebook or other social networking sites (unless my teacher said I could as part of a lesson)
- use chat rooms
- open any attachments in emails, or click any links in emails, without checking with a teacher first
- use mean or rude language when talking to other people online or in emails
- share my password with others or log in using someone else's name or password
- bully other people

Also:

- I understand that the school will check the websites I visit and how I use the school's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules.
- I will tell a teacher or a member of staff I know immediately if I find anything on a school computer or online that upsets me, or that I know is mean or wrong.
- I will always be responsible when I use the School's ICT systems and internet.
- I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.

Signed (pupil):	**Date:**

Parent/carer agreement: I agree that my child can use the School's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the School's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):	**Date:**