Olive AP Academy
SUFFOLK
Olive Academies

Olive AP Academy – Suffolk

ICT & Online Safety Policy

This academy's online safety coordinator is Judy Lewis

Document control table	
Title	ICT & Online Safety Policy
Date updated and approved	25 August 2021
Approved by	OA EPS committee
Date of next review	July 2022
Updates/revisions included July 2021:	• Withdrawn COVID-19 note in line with KCSIE guidance • Updated areas of risk in line with KCSIE • Updated relevant legislation • Edited roles to highlight that DSL is responsible for online safety • Emphasised role of governance and oversight of online safety inline with KCSIE guidance • Added detail on RSE curriculum in relation to online safety • Updated definition of cyberbullying • Added reference to power to delete as well as search and confiscate (section 4) • All schools now use Schools Broadband and Senso filtering (section 5)
The structure of this policy is an OA central template, but it should be localised to each academy depending on ICT provision within the academy, and to provide local contacts. A final copy of the academy specific policy should be sent to OA central for filing and uploading on the website. **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 is part of the academy's statutory safeguarding policy. Any issues and concerns with online safety _must_ follow the academy's safeguarding and child protection processes.

Contents

1. Introduction and overview

Rationale

The purpose of this policy is to:

- set out the key principles expected of all members of this academy 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 today's and tomorrow's 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 academy community.
- have clear structures to deal with online abuse such as online bullying [noting that these need to be cross referenced with other academy policies]
- ensure that all members of the academy 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 students.

The main areas of risk for our academy can be summarised as follows:

Content

- exposure to inappropriate content
- lifestyle websites promoting harmful behaviours
- hate content
- content validation: how to check authenticity and accuracy of online content.

Contact

- grooming (criminal, sexual exploitation, radicalisation etc.)
- online bullying in all forms
- social or commercial identity theft, including passwords.

Conduct

- aggressive behaviours, peer on peer abuse, cyberbullying
- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- child mental health and wellbeing (amount of time spent online, gambling, body image)
- sharing of sexual images (nude, semi-nude and pornographic) which constitute sexual violence and harm
- copyright (little care or consideration for intellectual property and ownership).

Scope

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

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

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 – a framework to equip children and young people for digital life – updated June 2020
- 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.

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) 2021 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 academy and the trust.

This policy complies with our funding agreement and articles of association.

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

- Safeguarding and child protection
- Anti-bullying
- Behaviour
- Relationships and sex education
- PSHE
- Data protection
- Staff code of conduct
- Staff use of social media

Roles and responsibilities

Role	Key responsibilities
OA MAT board (Education Performance and standards committee) & AAB advisory member (safeguarding)	KCSIE 2021 emphasis is placed, as part of the requirement, for staff to undergo regularly updated safeguarding training, including online safety (paragraph 101) and the requirement to ensure children are taught about safeguarding, including online safety (paragraph 106), that safeguarding training for staff, including online safety training, is integrated, aligned and considered as part of the whole school or college safeguarding approach. Whilst considering the above training requirements, regard should be given to the Teachers' Standards which set out the expectation that all teachers manage behaviour effectively to ensure a good and safe educational environment and requires teachers to have a clear understanding of the needs of all pupils. • To ensure that the academy has in place policies and practices to keep the children and staff safe online (EPS committee). • To approve the online safety policy and review the effectiveness of the policy (EPS committee). • To support the academy in encouraging parents and the wider community to become engaged in online safety activities (AAB member). • The role of the safeguarding AAB member will include: regular review with the online safety coordinator (where same as safeguarding lead).
Headteacher	• Must be adequately trained in off-line and online safeguarding, in-line with statutory guidance and guidance from the safeguarding children's partnership within the local area. • To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole academy safeguarding. • To take overall responsibility for online safety provision. • To take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and trustees to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information ensuring academy's provision follows best practice in information handling.

Role	Key responsibilities
	• To ensure the academy uses appropriate IT systems and services including, filtered Internet Service. • To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles. This includes at induction and is regularly updated for all staff. • To be aware of procedures to be followed in the event of a serious online safety incident. • Ensure suitable 'risk assessments' undertaken so the curriculum meets needs of pupils, including risk of children being radicalised. • To receive regular monitoring reports from the online safety coordinator. • To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures, e.g. network manager. • To ensure OA central and the Academy Advisory Board (AAB) are regularly updated on the nature and effectiveness of the academy's arrangements for online safety.
Designated Safeguarding Lead	• Take day to day responsibility for online safety issues and a leading role in establishing and reviewing the academy's online safety policy/documents. • Promote an awareness and commitment to online safety throughout the academy. • Ensure that online safety education is embedded within the curriculum. • To communicate regularly with headteacher, SLT and ICT manager to discuss current issues, review incident logs and filtering/change control logs. • To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident. • To ensure that online safety incidents are logged as a safeguarding incident. • ensure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy • Facilitate training and advice for all staff. • Oversee any pupil surveys / pupil feedback on online safety issues. • Liaise with other agencies and/or external services if necessary • Stay up to date with online safety issues and legislation and be aware of the potential for serious child protection concerns. • provide regular reports on online safety in school to the headteacher and AAB
Computing Curriculum lead (might be 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
PSHE/RSE lead	• As listed in the 'all staff' section, plus: • Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE and RSE curriculum

Role	Key responsibilities
	• Work closely with the DSL/ and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE and RSE
Network Manager/ technician	• To put in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material. • To report online safety related issues that come to their attention, to the DSL. • To conduct a full security check and monitor the school's ICT systems twice a year • To block access to potentially dangerous sites and, where possible, prevent the download of potentially dangerous files • To manage the academy's computer systems, ensuring academy password policy is strictly adhered to. • Keep up to date with this policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
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 academy must be registered with Information Commissioner by OA central.
Teachers	• To embed online safety in the curriculum. • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended academy activities if relevant). • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.
All staff	• To read, understand, sign and adhere to the academy acceptable use agreement which is contained within the annual staff declaration, and understand any updates annually. The staff declaration must be signed by new staff on induction. • To report any suspected cyberbullying, misuse or problem to the DSL. • To maintain an awareness of current online safety issues and guidance e.g. through CPD. • To model safe, responsible and professional behaviours in their own use of technology. **Exit strategy** • At the end of the period of employment to return any equipment or devices loaned by the academy. This will include leaving PIN numbers, IDs and

Role	Key responsibilities
	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 academy's ICT systems and internet – in the acceptable use agreement. • to consult with the academy if they have any concerns about their children's use of technology. • to support the academy in promoting online safety and endorse the pupil's acceptable use agreement which includes the pupils' use of the internet and the academy'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 academy'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.

Communication:

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

- policy to be posted on the academy website
- policy to be part of academy induction pack for new staff
- regular updates and training on online safety for all staff
- acceptable use agreements discussed with staff at the start of each year which expects staff to have read and understood this policy
- acceptable use agreements to be issued to students and parents on admission or at the start of the year depending on when the student is placed in the academy (see appendix 3).

Reviewing and monitoring this policy

- The online safety policy will be reviewed annually or when any significant changes occur regarding the technologies in use within the academy.
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by the Trust's Education Performance and Standards committee and seen by the AAB. All amendments to the academy online safety policy will be disseminated to all members of staff and pupils.

2. Education and curriculum

The following subjects have the clearest online safety links:

- PSHE
- Relationships and sex education
- Computing
- Citizenship

However, it is the role of all staff to identify opportunities to thread online safety through all activities, both outside the classroom and within the curriculum, supporting curriculum leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in the academy or setting as homework tasks, all staff should encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites (ask your DSL what appropriate filtering and monitoring policies are in place).

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law. saferesources.lgfl.net has regularly updated theme-based resources, materials and signposting for teachers and parents.

Students in **Key Stage 2** will be taught to:

- use technology safely, respectfully and responsibly
- recognise acceptable and unacceptable behaviour
- identify a range of ways to report concerns about content and contact.

In line with guidance on RSE education, by the end of **primary school** pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

In **Key Stage 3**, students 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.

Students 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.

In line with the RSE curriculum, 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 academy 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.

Parent awareness and training

This academy provides online advice and information for parents through its website, and on an ongoing basis. 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

3. Handling online safety and cyberbullying concerns and incidents

It is vital that all staff recognise that online safety is a part of safeguarding as well as the curriculum.

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 contribute 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).

Academy procedures for dealing with online safety are detailed in:

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Behaviour Policy
- Acceptable Use Policies
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)

OA commits to take all reasonable precautions to ensure online safety but recognises that incidents will occur both inside and outside the academy (and that those from outside the academy will continue to impact on pupils when they come into the academy. All members of the academy are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the academy'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, unless the concern is about the headteacher in which case the compliant is referred to the CEO and the LADO (Local Authority's Designated Officer). 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 (particular procedures are in place for sexting; see section below).

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 academy treats bullying and procedures in place to support students who are bullied and who bully.

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

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

Where a student misuses the academy'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 academy'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 academy will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Social media incidents

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

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

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the academy 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 academy 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.

4. Searching, deletion and confiscation

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the headteacher and staff authorised by them have the right to search pupils' phones, computers or other devices for pornographic images or any other data or items banned under school rules or legislation. This includes the content of mobile phones and other devices, for example as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying.

The school can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the school's rules.

Full details of the academy's search procedures are available in the OA's Behaviour policy and anti-bullying policies.

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

5. Managing IT and communication system

Internet access, security (virus protection) and filtering

This academy:

- informs all users that Internet/email use is monitored
- has the educational filtered secure broadband connectivity through Schools Broadband
- uses 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
- uses USO user-level filtering where relevant
- ensures network health through use of Sophos anti-virus/anti-malware software
- Uses Microsoft office encrypted email service to send 'protect-level' (sensitive personal) data over the Internet
- Uses encrypted devices or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site;
- Works in partnership with the local authority to ensure any concerns about the system are communicated so that systems remain robust and protect students.

Network management (user access, backup)

This academy:

- uses individual, audited log-ins for all users
- uses guest accounts occasionally for external or short-term visitors for temporary access to appropriate services;
- uses teacher 'remote' management control tools for controlling workstations/viewing users/setting-up applications and Internet web sites, where useful;
- requires the technical support provider to be up-to-date with Thurrock Council services and policies;
- has daily back-up of academy data (admin and curriculum);
- uses secure, 'Cloud' storage for data back-up that conforms to DfE guidance;
- storage of all data within the academy 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, this academy:

- ensures staff read and sign that they have understood the academy'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. We also provide a different/use the same username and password for access to our academy's network
- ensures all pupils can access their individual accounts and store all work onto the student area;
- makes 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
- has 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

- requires all users to log off when they have finished working or are leaving the computer unattended
- ensures all equipment owned by the academy and/or connected to the network has up to date virus protection
- makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the academy, is used to support their professional responsibilities
- maintains equipment to ensure health and safety is followed
- ensures that access to the academy's network resources from remote locations by staff is audited and restricted and access is only through academy approved systems
- does 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
- has a clear disaster recovery system in place that includes a secure, remote off site back up of data
- this academy uses secure data transfer; this includes DfE secure S2S website for all CTF files sent to other schools
- ensures that all pupil level data or personal data sent over the Internet is encrypted and only sent through ARBOR or encrypted email
- our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- all IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards;

Password policy

- This academy makes it clear that staff and pupils must always keep their passwords private, must not share with others; If a password is compromised the academy should be notified immediately.
- All staff have their own unique username and private passwords to access academy 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.

Email

This academy:

- provides 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
- uses a number of technologies to help protect users and systems in the academy, including desktop anti-virus and anti-malware product Sophos, plus direct email filtering for viruses.

Students:

- To ensure OA has in place an effective remote learning programme (see below), students 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.
- Students are taught about the online safety and ‘etiquette’ of using email both in the academy and at home.

Staff:

- Staff can only use the Olive Academies email systems on the academy system
- Staff will use OA email systems for professional purposes
- Access in the academy to external personal email accounts may be blocked
- Never use email to transfer staff or pupil personal data. ‘Protect-level’ data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption.

Academy 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 academy’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 academy website.

Remote learning tools and systems

Given the COVID-19 pandemic there is a need for schools to ensure a remote learning contingency plan is in place for pupils who cannot attend school. Any online learning tools and systems that are used including virtual lessons are in line with privacy and data protection requirements and mirror the principles outlined in this policy.

Guidance will be provided to teaching staff, students and parents about procedures for ensuring safety for all when delivering remote education. Considerations include:

- Check settings and ensure that you are aware of what permissions are available to you as a host and which are available to pupils/parents at their home
- Ensure as host, you are in control of the screen controls, i.e. who can control the screen
- Learn how to mute and unmute all participants, including video screens
- No 1:1s, groups only
- Staff and children must wear suitable clothing, as should anyone else in the household.
- Any computers used should be in appropriate areas, for example, not in bedrooms; and the background should be blurred.
- The live class should be recorded so that if any issues were to arise, the video can be reviewed.
- Live classes should be kept to a reasonable length of time, or the streaming may prevent the family ‘getting on’ with their day.
- Language must be professional and appropriate, including any family members in the background.
- Staff must only use platforms provided by Olive Academies to communicate with pupils

- Staff should record, the length, time, date and attendance of any sessions held.

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

Cloud environments

- Uploading of information on the academy'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 academy's online environment will only be accessible by members of the academy community;
- In the academy, pupils are only able to upload and publish within academy approved 'Cloud' systems.

CCTV

- We have CCTV in the academy as part of our site surveillance for staff and student safety. The use of CCTV is clearly signposted in the academy. 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.

6. Data security: Management Information System access and data transfer

Strategic and operational practices

At this academy:

- 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

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 academy-owned hardware will be recorded in a hardware inventory.
- Details of all academy-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.

7. Equipment and digital content

Mobile devices (mobile phones, tablets and other mobile devices)

- Mobile devices brought into the academy are entirely at the staff member, students & parents or visitors' own risk. The academy accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into academy.
- Mobile devices are not permitted to be used in certain areas within the academy site, e.g. changing rooms and toilets. 'Mobile-free' signs to this effect are displayed.
- The Bluetooth or similar function of a mobile device should not be used to send images or files to other mobile devices.
- No images or videos should be taken on mobile devices without the prior consent of the person or people concerned.
- All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any personal mobile device is to be avoided, except where it has been explicitly agreed by the headteacher. Such authorised use is to be recorded. 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 academy reserves the right to search the content of any mobile devices on the academy premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying.

Students' use of personal devices

- Pupil personal mobile devices, which are brought into the academy, must be turned off (not placed on silent) and handed to the academy office to be stored in a secure cabinet.
- 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 academy's behaviour policy. We reserve the right to use search devises such as security wands to identify students carrying mobile phones in contradiction with the acceptable use agreement.
- If a student needs to contact his or her parents or carers, they will be allowed to use an academy phone. Parents are advised not to contact their child via their mobile phone during the academy day, but to contact the academy office.

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 academy phone or landline.
- Staff will be issued with an academy phone where contact with students, parents or carers is required, for instance for off-site activities.

- Mobile phones and personally-owned devices will be switched off or switched to 'silent' mode. Mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity, then it will only take place when approved by the senior leadership team.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the academy office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.
- In an emergency where a staff member doesn't have access to an academy-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 academy 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.

Digital images and video

In this academy:

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the academy agreement form when their child joins the academy;
- We do not use first names to identify students 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 student photos (not group photos) are used on the academy website, in the prospectus or in other high profile publications the academy will obtain individual parental or pupil permission for its long term, high profile use;
- Staff sign the academy'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 students;
- Students are taught about how images can be manipulated in their online safety education programme and also 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;
- Students 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.
- Students 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

Appendix 1 – Good practice guidance on the use of images

This guidance covers the use of images on:

- Academy websites
- Social Media channels (Twitter, LinkedIn, Facebook etc.)
- Academy 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 academy 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 worn at all times.
- 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.

Photographs taken by parents at academy events

The academy 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 academy equipment, which should not leave the academy.

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 academy 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

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 academy?	
Do you know what you must do if a student approaches you with a concern or issue?	
Are you familiar with the academy’s acceptable use agreement for staff (contained within the annual staff declaration)?	
Are you familiar with the academy’s acceptable use agreement for pupils and parents (contained within the home academy agreement?	
Do you regularly change your password for accessing the academy’s ICT systems?	
Are you familiar with the academy’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.	

Appendix 3: Acceptable use agreements

3.1 Acceptable use agreement for parents and carers

Olive Academies

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 academy uses the following channels:

- our official Twitter account
- email/text groups for parents (for school announcements and information)
- our virtual learning platform Microsoft Teams (planned from September 2020)

Parents/carers also set up independent channels to help them stay on top of what's 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, the academy's Twitter account or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues if they aren't raised in an appropriate way
- use private groups, the academy's Twitter account 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:**

3.2 Acceptable use agreement for older pupils

Olive Academies

Acceptable use of the academy’s ICT facilities and internet: agreement for pupils and parents/carers

Name of pupil:

When using the academy’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

I understand that the school will monitor the websites I visit and my use of the academy’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 academy’s ICT systems and internet responsibly.

I understand that the academy 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 academy’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 academy’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:**

3.3 Acceptable use agreement for younger pupils

Olive Academies

Acceptable use of the academy’s ICT facilities and internet: agreement for pupils and parents/carers	
Name of pupil:	
When I use the academy’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 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 academy’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 academy’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 academy’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:**