Olive AP Academy
THURROCK

Olive Academies

Olive AP Academy – Thurrock

Online Safety Policy

Document control table	
Title	Online Safety Policy
Date approved	June 17
Approved by	OA EPS committee
Date of next review	June 18
Updates/revisions included:	
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 to be used by all OA pupils and staff.	

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

Useful information

Guidance on responding to online safety incidents
http://www.digitallyconfident.org/images/resources/first-line-information-support-HQ.pdf - page 23 onwards

Data security: Use of IT systems and Data transfer

Search and Confiscation guidance from DfE
https://www.gov.uk/government/publications/searching-screening-and-confiscation

1. Introduction and overview

Rationale

The purpose of this policy is to:

- set out the key principles expected of all members of the academy at Olive AP Academy – Thurrock (OA-Th) with respect to the use of IT-based technologies.
- safeguard and protect the 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 (sexual exploitation, radicalisation etc.)
- online bullying in all forms
- social or commercial identity theft, including passwords

Conduct

- aggressive behaviours (bullying)
- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online, gambling, body image)
- sexting
- 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.

Roles and responsibilities

Role	Key responsibilities
Headteacher	• Must be adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance • 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 (SIRO) ensuring academy's provision follows best practice in information handling • 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 • 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 • To ensure academy website includes relevant information.
Online safety coordinator/Designated Safeguarding Lead (This may be the same person)	• 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 • Liaise with academy technical staff where appropriate • To communicate regularly with SLT and the designated online safety LGB member 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 • Facilitate training and advice for all staff • Oversee any pupil surveys / pupil feedback on online safety issues • Liaise with the Local Authority and relevant agencies • Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection concerns.
OA MAT board (Education Performance and	• To ensure that the academy has in place policies and practices to keep the children and staff safe online (EPS committee)

Role	Key responsibilities
standards committee) & AAB advisory member (safeguarding)	• 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 online safety AAB member will include: regular review with the online safety coordinator (where same as safeguarding lead).
Computing Curriculum lead (might be QTLA lead)	• To oversee the delivery of the online safety element of the computing curriculum
Network Manager/technician	• To report online safety related issues that come to their attention, to the online safety coordinator • To manage the academy's computer systems, ensuring - academy password policy is strictly adhered to. - systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date) - access controls/encryption exist to protect personal and sensitive information held on academy-owned devices - the academy's policy on web filtering is applied and updated on a regular basis • That they keep up to date with the academy's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant • That the use of academy technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the online safety coordinator/headteacher • To ensure appropriate backup procedures and disaster recovery plans are in place • To keep up-to-date documentation of the academy's online security and technical procedures
Senior Information Risk Officer, Data and Information (Asset Owners) Managers (IAOs), e.g. business manager	• To ensure that the data they manage is accurate and up-to-date • 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. • 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

Role	Key responsibilities
All staff, volunteers and contractors.	• To read, understand, sign and adhere to the academy Acceptable Use Agreement/Policy, and understand any updates annually. The AUP is signed by new staff on induction. • To report any suspected misuse or problem to the online safety coordinator • 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/volunteering to return any equipment or devices loaned by the academy. 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.
Pupils	• Read, understand, sign and adhere to the Pupil Acceptable Use Policy annually • To understand the importance of reporting abuse, misuse or access to inappropriate materials • To know what action to take if they or someone they know feels worried or vulnerable when using online technology • To understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out of academy and realise that the academy's online safety policy covers their actions out of academy • To contribute to any 'pupil voice' / surveys that gathers information of their online experiences
Parents/carers	• To read, understand and promote the academy's Pupil Acceptable Use Agreement with their child/ren • 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.
External groups including parent groups	• Any external individual/organisation will sign an Acceptable Use agreement prior to using technology or the Internet within the academy • to support the academy in promoting online safety • To model safe, responsible and positive behaviours in their own use of technology.

Communication:

The policy will be communicated to staff/pupils/community in the following ways:

- policy to be posted on the academy website, academy office and in the staff room
- 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.
- 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 academy.

Handling incidents:

- The academy will take all reasonable precautions to ensure online safety.
- Staff and pupils are given information about infringements in use and possible sanctions.
- The online safety coordinator acts as first point of contact for any incident.
- Any suspected online risk or infringement is reported to online safety coordinator that day
- Any concern about staff misuse is always referred directly to the headteacher, unless the concern is about the headteacher in which case the complaint is referred to the OA Chief Executive and the LADO (Local Authority's Designated Officer).

Handling a sexting / nude selfie incident:

UKCCIS "Sexting in schools and colleges" should be used. This extract gives the initial actions that should be taken:

There should always be an initial review meeting, led by the DSL. This should consider the initial evidence and aim to establish:

- Whether there is an immediate risk to a young person or young people
  When assessing the risks the following should be considered:
  - Why was the imagery shared? Was the young person coerced or put under pressure to produce the imagery?
  - Who has shared the imagery? Where has the imagery been shared? Was it shared and received with the knowledge of the pupil in the imagery?
  - Are there any adults involved in the sharing of imagery?
  - What is the impact on the pupils involved?
  - Do the pupils involved have additional vulnerabilities?
  - Does the young person understand consent?
  - Has the young person taken part in this kind of activity before?
- If a referral should be made to the police and/or children's social care
- If it is necessary to view the imagery in order to safeguard the young person – in most cases, imagery should not be viewed
- What further information is required to decide on the best response
- Whether the imagery has been shared widely and via what services and/or platforms. This may be unknown.
- Whether immediate action should be taken to delete or remove images from devices or online services
- Any relevant facts about the young people involved which would influence risk assessment

- If there is a need to contact another academy, college, setting or individual
- Whether to contact parents or carers of the pupils involved - in most cases parents should be involved

An immediate referral to police and/or children's social care should be made if at this initial stage:

1. The incident involves an adult
2. There is reason to believe that a young person has been coerced, blackmailed or groomed, or if there are concerns about their capacity to consent (for example owing to special educational needs)
3. What you know about the imagery suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
4. The imagery involves sexual acts and any pupil in the imagery is under 13
5. You have reason to believe a pupil or pupil is at immediate risk of harm owing to the sharing of the imagery, for example, the young person is presenting as suicidal or self-harming

If none of the above apply, then the academy may decide to respond to the incident without involving the police or children's social care (an academy can choose to escalate the incident at any time if further information/concerns come to light).

The decision to respond to the incident without involving the police or children's social care would be made in cases when the DSL is confident that they have enough information to assess the risks to pupils involved and the risks can be managed within the academy's pastoral support and disciplinary framework and if appropriate local network of support.

Reviewing and monitoring online safety

The online safety policy is referenced within other academy policies (e.g. safeguarding policy, anti-bullying policy).

- The online safety policy will be reviewed annually or when any significant changes occur with regard to 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 MAT'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

Pupil online safety curriculum

This academy:

- has a clear, progressive online safety education programme as part of the computing curriculum/PSHE and other curriculum areas as relevant. This covers a range of skills and behaviours appropriate to their age and experience;
- plans online use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- will remind students about their responsibilities through the pupil Acceptable Use Agreement(s);
- ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright;
- ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
- ensure pupils only use academy-approved systems and publish within appropriately secure / age-appropriate environments.

Staff training

This academy:

- makes regular training available to staff on online safety issues and the academy's online safety education program;
- provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the online safety policy and the academy's Acceptable Use Agreements.

Parent awareness and training

This academy:

- provides online advice and information for parents through its website, and on an ongoing basis

3. Expected conduct and incident management

Expected conduct

In this academy, all users:

- are responsible for using the academy IT and communication systems in accordance with the relevant Acceptable Use Agreements;
- understand the significance of misuse or access to inappropriate materials and are aware of the consequences;

- understand it is essential to reporting abuse, misuse or access to inappropriate materials and know how to do so;
- understand the importance of adopting good online safety practice when using digital technologies in and out of the academy;
- know and understand academy policies on the use of mobile and hand held devices including cameras;

Staff, volunteers and contractors

- know to be vigilant in the supervision of children at all times, as far as is reasonable, and use common-sense strategies in learning resource areas where older pupils have more flexible access;
- know to take professional, reasonable precautions when working with pupils, previewing websites before use; using age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils;

Parents/Carers

- should provide consent for pupils to use the internet, as well as other technologies, as part of the online safety acceptable use agreement form;
- should know and understand what the academy 'rules of appropriate use for the whole academy' are and what sanctions result from misuse.

Incident management

In this academy:

- there is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions;
- all members of the academy are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the academy's escalation processes;
- support is actively sought from other agencies as needed (e.g. the local authority, E2BN, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, IWF) in dealing with online safety issues;
- monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the academy;
- parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible;
- the police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law;
- we will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform the LA.

4. 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 E2BN;
- uses the Smoothwall 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 software;
- Uses Microsoft Office 365 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 Thurrock Council and E2BN 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 - the Smoothwall USO system;
- 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 E2BN 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 EU and UK data protection requirements; Storage of data online, will conform to the 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 access the NSTUDENT account 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 to change their passwords into the MIS, E2BN USO admin site every 90 days
- 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 product Sophos, plus direct email filtering for viruses.

Pupils:

- We currently do not use pupil email systems. Should this be initiated, they will be intentionally 'anonymised' for pupil protection.
- Pupils are taught about the online safety and 'netiquette' of using e-mail 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. We do not use pupils' names when saving images in the file names or in the tags when publishing to the academy website.

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.

Social networking

Staff, volunteers and contractors

- Staff are instructed to always keep professional and private communication separate.
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the academy's preferred system for such communications.
- the use of any academy approved social networking will adhere to the academy's code of conduct.

Academy staff will ensure that in private use:

- No reference should be made in social media to students/pupils, parents/carers or academy staff;
- Academy staff should not be online friends with any pupil/student. Any exceptions must be approved by the headteacher.
- They should not be online friends with any pupil/student who have ever been a pupil at the academy
- They do not engage in online discussion on personal matters relating to members of the academy community;

- Personal opinions should not be attributed to the academy and personal opinions must not compromise the professional role of the staff member, nor bring the academy into disrepute;
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Staff should be aware that there is always a level of risk involved in having a personal social media account, and that it is their responsibility to manage it in a responsible way to minimise risk to personal privacy. The only way to ensure complete privacy, security and protection from any safeguarding allegation is to make a decision not to have any social media accounts.

Academy staff responsible for professional OA social media accounts will ensure:

- pupils' names are not used with their image on social media
- parental and pupil consent has been obtained to use pupils' photographs
- if sharing pupil's work use first names only and do not use an accompanying photograph
- personal, identifying information about pupils is never shared
- care is taken when tweeting about school trips – consider doing so after the event to prioritise pupils' safety
- social media tweets/posts are not derogatory or bring academy name into disrepute – no controversial personal views
- professional boundaries are maintained – don't follow pupils' individual twitter accounts or 'direct message' (DM) them
- you have permission to share material and acknowledge accordingly
- group photos are always preferable to single close-up images
- spellings are checked and that you think before you tweet. Consider your audience and don't say anything on Twitter that you wouldn't say face-to-face.
- social media is used as a 'broadcast' service to put information out about events, deadlines, emergency closures and to celebrate pupils' achievements
- academies engage with the local community and retweet relevant events.

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

Pupils:

- are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- are required to sign and follow our pupil Acceptable Use Agreement.

Parents:

- are reminded about social networking risks and protocols through our parental Acceptable Use Agreement and additional communications materials when required.
- are reminded that they need to ask permission before uploading photographs, videos or any other information about other people.

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

Strategic and operational practices

At this academy:

- The headteacher is the Senior Information Risk Officer (SIRO) (see section 1 – roles and responsibilities).
- Staff are clear who are the key contact(s) for key academy information (the Information Asset Owners) are. As outlined in section 1, the role of the IAO is to understand what information is held and for what purposes, who has access to it, and how it will be retained and disposed off.
- 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 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.

6. 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 be switched off at all times and 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.
- 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. Staff mobiles devices may be searched at any time as part of routine monitoring.

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.
- 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 or School Improvement 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. Bluetooth communication should be 'hidden' or switched off and 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.
- If a member of staff breaches the academy policy then disciplinary action may be taken.

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 daughter/son joins the academy;
- We do not identify pupils in online photographic materials or include the names of pupils in the credits of any published academy produced video materials/DVDs;

- Staff sign the academy's Acceptable Use Policy and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils;
- If specific pupil photos (not group photos) are used on the academy web site, 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
- The academy blocks/filter access to social networking sites unless there is a specific approved educational purpose;
- Pupils 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;
- 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.

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.

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. Best practice is to only use first names when possible (and never use a pupil's full name on social media).
-An exception to naming a child would be if a pupil was receiving an award, 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.

If you need further advice on working with the media please contact OA's Communications Executive Flora Jenkins on 01273 573834 or email flora.jenkins@oliveacademies.org.uk.

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.

Olive Academies

KS3/4 Student/Pupil Acceptable Use Agreement

Olive AP Academy – Thurrock regularly reviews and updates all acceptable use agreements documents to ensure that they are consistent with the academy online safety policy, which can be found at http://apthurrock.oliveacademies.org.uk/safeguarding-e-safety/

These rules will help to keep everyone safe and to be fair to others. Academy systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies.

1. I will be a responsible user and stay safe when using the internet and other digital technology at the academy.
2. I will only use the academy's computers for appropriate academy activities and learning and I am aware that the academy can monitor my internet use.
3. I will not use academy systems and equipment for personal and recreational use unless I have permission.
4. I will keep my logins, IDs and passwords secret and change my password regularly.
5. I will not bring files into the academy or download files that can harm the academy network or be used to bypass academy security.
6. I will only edit or delete my own files and not view, or change, other people's files or user areas without their permission.
7. I will use the internet responsibly and will not visit websites that are inappropriate for the academy or my learning activities.
8. I understand that websites, blogs, videos and other online information can be biased and misleading, so I need to check sources.
9. I am aware that some websites, games, online shopping, file sharing and social networks have age restrictions and I should respect this.
10. I will only e-mail or contact people as part of learning activities.
11. The messages I send, or information I upload, will always be polite and sensible. I understand that all messages I send reflect on me and the academy.
12. I will be careful when opening files and attachments, checking for viruses etc. If I am unsure I will never open a file, hyperlink or any other attachment.
13. When using the internet, I will not download copyright-protected material (text, music, video etc.)
14. I will not share my or others' personal information that can be used to identify me, my family or my friends on any online space, unless a trusted adult has given permission or reviewed the site.

15. I will never arrange to meet someone I have only ever previously met on the internet or by e-mail or in a chat room, unless I take a trusted adult with me.
16. I will only use my personal devices (mobile phones, USB devices etc.) in the academy if I have been given permission to do so.
17. I am aware that my online activity at all times should not upset or hurt other people and that I should not put myself at risk.
18. If I see anything I am unhappy with or I receive a message that makes me feel uncomfortable, I will not respond to it but I will save it and talk to a trusted adult.

I have read and understand these rules and agree to them.

Signed: _____ Date:_____

Olive Academies

Acceptable Use Agreement: all staff

Covers use of all digital technologies in the academy: i.e. **email, Internet, intranet, network resources,** learning platform, software, communication tools, social networking tools, academy website, **equipment and systems.**

Olive AP Academy - Thurrock regularly reviews and updates all acceptable use documents to ensure that they are consistent with the academy online safety policy.

These rules will help to keep everyone safe and to be fair to others. Academy systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies.

- I will only use the academy's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the headteacher and OA central.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password and change my passwords regularly. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other academy systems.
- I will ensure all documents, data, etc. are printed, saved, accessed and deleted / shredded in accordance with the academy's network and data security protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved email system(s) for any academy business.
- I will only use the academy approved communication systems with pupils or parents/carers, and only communicate with them on appropriate academy business.
- I will not support or promote extremist organisations, messages or individuals.
- I will not give a voice or opportunity to extremist visitors with extremist views.
- I will not browse, download or send material that is considered offensive or of an extremist nature by the academy.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the online safety coordinator.

- I will not download any software or resources from the internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.
- I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.
- I will not connect any device (including USB flash drive), to the network that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the academy's recommended anti-virus and other ICT 'defence' systems.
- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home or on any personal devices.
- I will follow the academy's policy on use of mobile phones / devices at the academy.
- I will only use academy approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the appropriate system or staff-only drive within the academy.
- I will only I take or publish images of staff and students with their permission and in accordance with the academy's policy on the use of digital / video images. Images published on the academy website, social media, online learning environment etc. will not identify students by name, or other personal information.
- I will use the academy's Learning Platform or online cloud storage service in accordance with academy protocols.
- I will ensure that any private social networking sites / blogs, etc. that I create or actively contribute to are not confused with my professional role.
- I will ensure, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role.
- I agree and accept that any computer or laptop loaned to me by the academy, is provided solely to support my professional responsibilities and that I will notify the academy of any "significant personal use" as defined by HM Revenue & Customs.
- I will only access academy resources remotely (such as from home) using academy approved system and follow e-security protocols to interact with them.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow academy data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the academy's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will alert the academy's Designated Safeguarding Lead or an appropriate senior member of staff if I feel the behaviour of any child may be a cause for concern.

- I understand it is my duty to support a whole-academy safeguarding approach and will report any behaviour of other staff or pupils, which I believe may be inappropriate or concerning in any way, to the DSL.
- I understand that all internet and network traffic / usage can be logged and this information can be made available to the Head or Safeguarding Lead on their request.
- I understand that Internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.
- I will only use any local authority system I have access to in accordance with their policies.
- *Staff that have a teaching role only:* I will embed the academy's on-line safety / digital literacy / counter extremism curriculum into my teaching.

User signature

I agree to abide by all the points above.

I understand that I have a responsibility for my own and others' online safety and I undertake to be a 'safe and responsible digital technologies user'.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the academy's most recent online safety / safeguarding policies.

I understand that failure to comply with this agreement could lead to disciplinary action.

Signature ..... Date .....

Full Name ..... (printed)

Job title / Role .....

Authorised Signature (Headteacher / Deputy)

I approve this user to be set-up on the academy systems relevant to their role

Signature ..... Date.....

Full Name ..... (printed)