ADVANCE LEARNING PARTNERSHIP

E-Safety Policy

Date: September 2025
Review Date: September 2027

Relating to all Academies of the
Advance Learning Partnership Multi Academy Trust

Contents

Policy Links

This policy coordinates with:

- Safeguarding Policy
- Behaviour Policy
- Staff disciplinary Policy
- Data Protection Policy
- Privacy Notices
- Online Safety Policy

This E-Safety Policy recognises the commitment of our Trust to E-Safety and acknowledges its part in the Trust's overall Safeguarding policies and procedures. It shows our commitment to meeting the requirement to keep pupils safe when using technology. We believe the whole Trust community can benefit from the opportunities provided by the Internet and other technologies used in everyday life. The E-Safety policy supports this by identifying the risks and the steps we are taking to avoid them.

Our expectations for responsible and appropriate conduct are formalised in this policy which we expect all staff and pupils to follow.

The scope of policy

- This policy applies to the whole Trust community including the senior leadership teams (SLT), Trustees/Governors, all staff employed directly or indirectly by the Trust, visitors and all pupils.

- The senior leadership team and Trustees/Governors, and will ensure that any relevant or new legislation that may impact upon the provision for E-Safety within school will be reflected within this policy.

- The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber bullying, or other E-Safety-related incidents covered by this policy, which may take place out of school but is linked to membership of the school.

- The Education Act 2011 gives the school the power to confiscate and search the contents of any mobile device if the Headteacher believes it contains any material that could be used to bully or harass others. The Searching, screening and confiscation at school (DfE, January 2018) states staff may lawfully search electronic devices, without consent or parental permission, if there is a suspicion that the pupil has a device prohibited by school rules, or the staff member has good reason to suspect the device may be used to cause harm, disrupt teaching, commit an offence, break school rules, cause personal injury or to damage property.

- The school/Trust will clearly detail its management of incidents within this policy, associated Behaviour, Anti-Bullying and Online Safety Policies and will, where known, inform parents/carers of incidents of inappropriate E-Safety behaviour that take place out of school.

- It takes into account the DfE statutory guidance 'Keeping Children Safe in Education' , Early Years and Foundation Stage , 'Working Together to Safeguard Children' and the Durham Safeguarding Children's Partnership procedures.

Implementation of the policy

- The senior leadership team will ensure all members of school staff are aware of the contents of the school E-Safety Policy and the use of any new technology within school.
- All amendments will be published and awareness sessions will be held for all members of the school community.
- E-Safety will be taught as part of the curriculum in an age-appropriate way to all pupils.
- E-Safety posters will be prominently displayed around the school.
- The E-Safety Policy will be made available to parents, carers and others via the website.

Responsibilities of the School Community

We believe that E-Safety is the responsibility of the whole Trust community and that everyone has their part to play in ensuring all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

The Senior Leadership Team accepts the following responsibilities:

- The Headteacher will take ultimate responsibility for the E-Safety of the school community.
- Identify a person to take day to day responsibility for E-Safety; provide them with training; monitor and support them in their work.
- Ensure adequate technical support is in place to maintain a secure ICT system.
- Ensure policies and procedures are in place to ensure the integrity of the school's information and data assets.
- Ensure liaison with the Governors.
- Develop and promote an E-Safety culture within the school community.
- Ensure that all staff, pupils and other users agree to the Acceptable Use Policy and that new staff have E-Safety included as part of their induction procedures.
- Make appropriate resources, training and support available to all members of the school community to ensure they are able to carry out their roles effectively with regard to E-Safety.
- Receive and regularly review E-Safety incident logs; ensure that the correct procedures are followed should an E-Safety incident occur in school and review incidents to see if further action is

required. (E-Safety incidents will be recorded for all students on CPOMS and any incidents involving staff will be dealt with under the relevant HR Policy).

Responsibilities of all Staff:

- Read, understand and help promote the school's E-Safety Policies and guidance.
- Read, understand and adhere to the staff Acceptable Use Policy (AUP).
- Take responsibility for ensuring the safety of sensitive school data and information.
- Develop and maintain an awareness of current E-Safety issues, legislation and guidance relevant to their work.
- Maintain a professional level of conduct in their personal use of technology at all times.
- Ensure that all digital communication with pupils is on a professional level and only through school based systems, NEVER through personal email, text, mobile' phone, social network or other online medium.
- Embed E-Safety messages in learning activities where appropriate.
- Supervise pupils carefully when engaged in learning activities involving technology.
- Ensure that pupils are told what to do should they encounter any material or receive a communication which makes them feel uncomfortable.
- Report all E-Safety incidents which occur in the appropriate log and/or to their line manager. Incident should be recorded using CPOMS.
- Respect, and share with pupils the feelings, rights, values and intellectual property of others in their use of technology in school and at home.
- Support the school in providing a safe technical infrastructure to support learning and teaching.
- Ensure appropriate technical steps are in place to safeguard the security of the school ICT system, sensitive data and information. Review these regularly to ensure they are up to date.
- Ensure that provision exists for misuse detection and malicious attack.
- At the request of the Leadership team conduct occasional checks on files, folders, email and other digital content to ensure that the Acceptable Use Policy is being followed.
- Report any E-Safety related issues that come to their attention to the E-Safety lead and/or senior leadership team.

- Ensure that procedures are in place for new starters and leavers to be correctly added to and removed from all relevant electronic systems, including password management.

- Ensure that suitable access arrangements are in place for any external users of the schools ICT equipment.
- Ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.

- Ensure staff are making use of the ICT systems to monitor and manage student's computer usage.

Responsibilities of pupils:

- Read, understand and adhere to the student AUP and follow all safe practice guidance.

- Take responsibility for their own and each other's safe and responsible use of technology wherever it is being used, including judging the risks posed by the personal technology owned and used by them outside of school.

- Ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home.

- Understand what action should be taken if they feel worried, uncomfortable, vulnerable or at risk whilst using technology, or if they know of someone to whom this is happening.

- Report all E-Safety incidents to appropriate members of staff.

- Discuss E-Safety issues with family and friends in an open and honest way.

- To know, understand and follow school policies on the use of mobile phones, portable devices, digital cameras and handheld devices.

- To be involved in the content delivered in school based on topical events as well as contribution towards items such as the student AUP.

Responsibilities of Parents/Carers:

- Help and support the school in promoting E-Safety.

- Read, understand and promote the pupil ICT agreement with their children.

- Discuss E-Safety concerns with their children, show an interest in how they are using technology and encourage them to behave safely and responsibly when using technology.

- Consult with the school if they have any concerns about their child's use of technology.

- To agree to and sign the home-school agreement and photo/video consent which clearly sets out the use of photographic and video images of pupils.

- Read, understand and adhere to the student AUP and follow all safe practice guidance.

- To keep up-to-date with topical e-safety issues and read updates from the schools' website "Internet safety" section and from the school's social networking page.

Responsibilities of Trustees/Governors:

- Read, understand, contribute to and help promote the school's E-Safety policies and guidance as part of the Trust's overarching Safeguarding procedures.

- Support the work of the school/Trust in promoting and ensuring safe and responsible use of technology in and out of school/Trust, including encouraging parents to become engaged in E-Safety awareness.
- To have an overview of how the school IT infrastructure provides safe access to the Internet and the steps the school takes to protect personal and sensitive data.

- Ensure appropriate funding and resources are available for the school to implement their E-Safety strategy.

Responsibilities of the Designated Safeguarding Lead:

- Understand and raise awareness of the issues and risks surrounding the sharing of personal or sensitive information.

- Be aware of and understand the risks to young people from online activities such as grooming for sexual exploitation, sexting, cyberbullying and others.

- Raise awareness of the particular issues which may arise for vulnerable pupils in the school's approach to E-Safety ensuring that staff know the correct child protection procedures to follow.

Teaching and Learning

We believe that the key to developing safe and responsible behaviours online for everyone within our Trust community lies in effective education. We know that the Internet and other technologies are embedded in our pupils' lives, not just in school but outside as well and we believe we have a duty to help prepare our pupils to benefit safely from the opportunities that these present.

We will deliver a planned and progressive scheme of work to teach E-Safety knowledge and understanding and to ensure that pupils have a growing understanding of how to manage the risks involved in online activity. We believe that learning about E-Safety should be embedded across the curriculum and also taught in specific lessons such as Computing.

We will deliver e-safety lessons to students outside of the Computing department via the PSHE / RSE programme where all school tutors will deliver a series of lessons on the topic of e-safety to all

students in the schools. Students will also have access to external visitors during whole and year group assemblies and advice given on the school's website in the "Internet safety" section.

We will teach pupils how to search for information and to evaluate messages with pupils routinely wherever suitable opportunities arise. This includes the need to protect personal information and to consider the consequences their actions may have on others. Staff will model safe and responsible behaviour in their own use of technology during lessons.

We will remind pupils about the responsibilities to which they have agreed through the AUP.

Pupils will be made aware of where to seek advice or help if they experience problems when using the Internet and related technologies.

How parents/carers will be involved

We believe it is important to help all our parents develop sufficient knowledge, skills and understanding to be able to help keep themselves and their children safe. To achieve this we will offer opportunities for finding out more information through meetings, the school newsletter, social media and website.

We ask parents to sign the ICT agreement which includes a statement about their use of social networks in situation where it could reflect on our school's reputation and on individuals within the school community.

We request our parents to support the school in applying the E-Safety Policy and keeping up-to-date with topical e-safety issues updated on the school website and social networking pages.

Filtering Internet access

Web filtering of Internet content is provided by Smoothwall. This ensures that all reasonable precautions are taken to prevent access to illegal content. However, it is not possible to guarantee that access to unsuitable or inappropriate material will never occur and we believe it is important to build resilience in pupils in monitoring their own Internet activity.

All users are informed about the action they should take if inappropriate material is accessed or discovered on a computer. However, deliberate access of inappropriate or illegal material will be treated as a serious breach of the AUP and appropriate sanctions taken.

We recognise that students should not just rely on filter web access but should also develop their own skills when deciding whether information and websites they are viewing are reliable or not.

Access to school systems

The school decides which users should and should not have Internet access, the appropriate level of access and the level of supervision they should receive. There are robust systems in place for managing network accounts and passwords, including safeguarding administrator passwords. Suitable arrangements are in place for visitors to the school who may be granted a temporary log in.

All users are provided with a log in appropriate to their key stage or role in school. Pupils are taught about safe practice in the use of their log in and passwords. Password procedures now require students to change their passwords more regularly and meet the schools defined complexity.

Access to personal, private or sensitive information and data is restricted to authorised users only, with proper procedures being followed for authorising and protecting login and password information.

Using the Internet

We provide the Internet to:

- Support curriculum development in all subjects;
- Support the professional work of staff as an essential professional tool;
- Enhance the school's management information and business administration systems;
- Enable electronic communication and the exchange of curriculum and administration data with the LA, the examination boards and others.

Users are made aware that they must take responsibility for their use of, and their behaviour whilst using the school IT systems or a school provided laptop or device and that such activity can be monitored and checked.

All users of the school IT or electronic equipment will abide by the relevant Acceptable Use Policy (AUP) at all times, whether working in a supervised activity or working independently.

Pupils and staff are informed about the actions to take if inappropriate material is discovered and this is supported by notices in classrooms and around school.

Using email

Email is regarded as an essential means of communication and the school provides all members of the school community with an e-mail account for school based communication.

Communication by email between staff, pupils and parents will only be made using the school email account and should be professional and related to school matters only. E-mail messages on school business should be regarded as having been sent on headed notepaper and reflect a suitable tone and content and should ensure that the good name of the school is maintained. There are systems in place for storing relevant electronic communications which take place between school and parents.

Use of the school e-mail system is monitored and checked.

Creating online content as part of the curriculum

As part of the curriculum we encourage pupils to create online content. Pupils are taught safe and responsible behaviour in the creation and publishing of online content. They are taught to publish for a wide range of audiences which might include governors, parents or younger children. Personal publishing of online content is taught via age-appropriate sites that are suitable for educational purposes. They are moderated by the school where possible. Pupils will only be allowed to post or

create content on sites where members of the public have access when this is part of a school related activity. Appropriate procedures to protect the identity of pupils will be followed.

We take all steps to ensure that any material published online is the author's own work, gives credit to any other work included and does not break copyright.

Remote Learning

ALP recognise that Remote Learning and use of webcams can be a challenging activity but brings a wide range of learning benefits. Remote Learning contact details will not be posted publicly, links to lessons should be shared via e-mail or through the schools VLE. Where possible staff will deliver any remote content from school. Staff will ensure that remote learning opportunities are suitable, risk assessed and use their school login details when conducting any remote learning.

Students should not instigate any video calls with staff. Remote Learning will take place via official and approved communication channels following a robust risk assessment.

When recording a remote lesson, it should be made clear to all parties at the start of the lesson and permission will be obtained from all participants; the reason for the recording must be given and recorded material will be stored securely. If third party materials are included, we will check that recording is permitted to avoid infringing the third-party intellectual property rights.

The following guides have been produced to support students and parents.

Using images, video and sound

We recognise that many aspects of the curriculum can be enhanced by the use of multi-media and that there are now a wide and growing range of devices on which this can be accomplished. Pupils are taught safe and responsible behaviour when creating, using and storing digital images, video and sound.

Digital images, video and sound recordings are only taken with the permission of participants and their parents; images and video are of appropriate activities and are only taken of pupils wearing appropriate dress. Full names of participants are not used either within the resource itself, within the file-name or in accompanying text online.

We ask all parents/carers to sign an agreement about taking and publishing photographs and videos of their children (in publications and on websites) and this list is checked whenever an activity is being photographed or filmed.

Students are also taught the implications of legislation such as the copyright law and computer misuse via their ICT lessons and through whole school assemblies.

Using Mobile phones and Social Media

With regards to use of mobile phones and social media please refer the Online Safety Policy.

Using other technologies

As a Trust we will keep abreast of new technologies and evaluate both the benefits for learning andteaching and also the risks from an E-Safety point of view.

We will regularly review the E-Safety Policy to reflect any new technology that we use, or to reflect the use of new technology by pupils.

Staff or pupils using a technology not specifically mentioned in this policy, or a personal device whether connected to the school network or not, will be expected to adhere to similar standards of behaviour to those outlined in this document.

Protecting school data and information

ALP recognises their obligation to safeguard staff and pupil's sensitive and personal data including that which is stored and transmitted electronically. We regularly review our practices and procedures to ensure that they meet this basic obligation.

Pupils are taught about the need to protect their own personal data as part of their E-Safety awareness and the risks resulting from giving this away to third parties.

ALP is a registered Data Controller under the General Data Protection Regulation (GDPR) and we comply at all times with the requirements of that registration. All access to personal or sensitive information owned by the school/Trust will be controlled appropriately through technical and non-technical access controls.

Responding to E-Safety incidents

Any incidents where pupils do not follow the Acceptable Use Policy will be dealt with following the school's normal behaviour or disciplinary procedures.

In situations where a member of staff is made aware of a serious E-Safety incident, concerning pupils or staff, they will inform the DSL, E-Safety Lead or Headteacher who will then respond in the most appropriate manner.

Instances of cyber bullying will be taken very seriously by the school and dealt with using the schools anti-bullying procedures. School recognises that staff as well as pupils may be the victims and will take appropriate action in either situation, including instigating restorative practices to support the victim.

School reserves the right to monitor equipment on their premises and to search any technology equipment, including personal equipment with permission, when a breach of this policy is suspected.

The school will follow the NPCC guidance on when to contact the Police available here: when-to-call-the-police--guidance-for-schools-and-colleges.pdf (npcc.police.uk)

If an incident or concern needs to be passed beyond our community (for example, if other local settings are involved or the public may be at risk), the DSL or Headteacher will speak with the Police first to ensure that potential investigations are not compromised.

Dealing with a Child Protection issue arising from the use of technology

If an incident occurs which raises concerns about Child Protection or the discovery of indecent images on the computer, then the procedures outlined in the Safeguarding Policy will be followed.

The following activities are likely to result in disciplinary action:

- Any online activity by a member of the school community which is likely to adversely impact on the reputation of the school;
- Accessing inappropriate or illegal content accidentally and failing to report this;
- Inappropriate use of personal technologies (e.g. mobile phones) at school or in lessons;
- Sharing files which are not legitimately obtained e.g. music files from a file sharing site;
- Using school or personal equipment to send a message, or create content, that is offensive or bullying in nature or could bring the school into disrepute;
- Attempting to circumvent school filtering, monitoring or other security systems;
- Circulation of commercial, advertising or 'chain' emails or messages;
- Revealing the personal information (including digital images, videos and text) of others by electronic means (e.g. sending of messages, creating online content) without permission;
- Using online content in such a way as to infringe copyright or which fails to acknowledge ownership (including plagiarizing of online content);
- Transferring sensitive data insecurely or infringing the conditions of GDPR.
- Accessing social networking sites, chat sites, instant messaging accounts, email or using a mobile phone for personal use during lesson time;
- Accessing non-educational websites (e.g. gaming or shopping websites) during lesson time;
- Sharing a username and password with others or allowing another person to log in using your account;
- Accessing school ICT systems with someone else's username and password;
- Deliberately opening, altering, deleting or otherwise accessing files or data belonging to someone else.

Safeguarding/Wellbeing

If a member of staff has any concerns in relation to the child's welfare/wellbeing the member of staff should log this on CPOMS and speak with Designated Safeguarding Lead, or appropriate team member. Further guidance can be found in the Safeguarding Policy.

Equality and Diversity

All developments are intended to ensure that no-one is treated in any way less favourably on the grounds of age, race, disability, gender reassignment, sexual orientation, sex, marriage & civil partnership, pregnancy & maternity, religion/ belief or political/ other personal beliefs.

Complaints

All complaints should be raised with the school in the first instance.

The details of how to make a formal complaint can be found in the School Complaints Policy.

Modern Slavery Act

Advance Learning Partnership (Trust) is committed to ensuring that modern slavery and human trafficking are prevented from taking place within the Trust and its supply chain.
The Trust is committed to sourcing responsibly and improving our practices to combat slavery and human trafficking in our business and supply chain.

Accessibility Statement

We are committed to ensuring that our policies are accessible to all individuals. If you require this policy document in an alternative format, such as Braille, large print, or another language, please do not hesitate to contact our office. Immersive Reader tools are a useful way for an enhanced reading experience. PDF and word have this as a function. Your accessibility needs are important to us, and we are here to assist you in any way possible.

Control of Documents - Records/Policies

Document Name	Staff Member
E-Safety Policy, including AUPs	Mike Carnaffin

Description	Name / Title	Signature	Date
Prepared by	Person who updated policy	M Carnaffin	19.05.2025
1st - Approved by	Person who approved policy	ELT	June 2025
2nd - Approved by (If more than 1 approver)	Second person who approved policy	Trust Board (ARC)	10.07.2025

Appendix 1. – Staff Acceptable Use Policy

Policy Overview

The Advance Learning Partnership (ALP) provides a wide variety of ICT equipment for use by staff as an important tool for teaching, learning, and administration of the school. Use of school ICT equipment, by members of staff, is governed at all times by this Acceptable Use Policy. Please ensure you understand your responsibilities under this policy, and direct any questions or concerns to a senior member of staff in the first instance.

All members of staff have a responsibility to use the school's ICT system(s) in a professional, lawful, and ethical manner. Deliberate abuse of the school's ICT system(s) may result in disciplinary action (including possible termination of employment) as well as possible civil and/or criminal liability.

This policy is not intended to limit arbitrarily the ways in which you can use the system(s), but to ensure compliance with the legal responsibilities of the school and staff, to safeguard the reputation of the school, and to ensure the safety of all users. Please respect these guidelines, many of which are in place for your protection.

The Staff AUP compliments the E-Safety/Online Safety Policy. Please ensure you have read and comply with guidance in the E-Safety Policy.

This Acceptable Use Policy is intended to ensure that:

- Staff and volunteers will be responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use.
- School systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- Staff are protected from potential risk in their use of technology in their everyday work.
- To ensure that staff will do their utmost to protect and educate the students in the Academy.

1. Policy Statement

1.1 The Advance Learning Partnership reserves the right to amend this Acceptable Use Policy, at any time, without notice. Once amended the revised policy will be circulated to all staff via email.It is your responsibility to ensure that you are up to date with such changes.

1.2 This Acceptable Use Policy replaces and supersedes all previous versions.

2. Access to the School Network

2.1 All new members of staff will partake in ICT induction at the start of their tenure. The training is designed to ensure correct usage of ICT equipment and network resources on site. The trainingwill also focus on safe use of electronic resources such as the Internet and email to ensure compliance with this document.

2.2 The ALP reserves the right to monitor user activity remotely. The ALP also reserves the rightto monitor all network traffic either manually or through automated software, to ensure policy compliance and to aid in resolving any issues.

2.3 Users should not allow any other person access to any equipment/device logged in under theirown user account, unless as part of authorised work. Allowing another person to use your credentials for any of the school ICT systems for any other reason is a severe breach of this Acceptable Use Policy and contravenes legislation.

2.4 It is imperative that members of staff protect their password(s) and computer(s) at all times. Staff should ensure passwords are a suitable complexity and change regularly in order to reduce unauthorised access.

2.5 Passwords and other credentials for any ICT system(s) must never be divulged to anyone at any time, doing so is a severe breach of this Acceptable Use Policy.

2.6 If it is suspected that a password has been compromised it must be changed immediately.

2.7 It is prohibited to copy any software or inappropriate material on to any network resource. Access to the school network and the school designated wireless networks is only granted to school workstations/laptops.

2.8 The use of network resources is a privilege and inappropriate use will result in that privilege being withdrawn and other action, as appropriate taken.

2.9 By storing or creating any personal documents or files on the school computer system, you grant the school a non-exclusive, universal, perpetual, irrevocable, and royalty-free license to use, copy, and distribute those documents or files in any way the school sees fit.

3. Home Directories / Work Areas

3.1 Each member of staff will have access to a Home Directory located on the school file server.

3.2 The ALP reserves the right to delete and report to the Senior Leadership Team any inappropriate materials found within staff Home Directories during any routine or random checks. Inappropriate materials include but are not limited to:

- Pornographic Material (of either a legal or illegal nature)
- Material which incites hatred or discrimination
- Material which promotes illegal activity
- Material which is in breach of the GDPR
- Material which is degrading to persons or groups of persons

3.3 Staff must always check all files brought in on removable media (such media includes but is not limited to USB Flash Drives, External Hard Drives, Memory Cards, Cloud based storage etc.) with the Antivirus software installed on site.

3.4 Removable media should only be used if it is found to be free of any virus. All incidents of infection through a Virus, Trojan or Spyware should be reported to the ICT Support and Development Team immediately.

3.5 Staff should ensure that worked deemed to be important is copied onto their work area in order for the school's backup system to replicate this.

4. Electronic Mail

4.1 All members of staff will be provided with a school email address from the Office 365 platform or other mail program.

4.2 Members of staff are responsible for all the e-mails they send, for any contacts made and for ensuring that their mailbox is kept within the allocated quota which is currently set to 1GB for all members of staff.

4.3 Caution should be exercised when sending confidential information via e-mail to external recipients. Any documents sent via email containing personal or sensitive information must be password protected and the password must be sent over a separate communication channel, e.g. by disclosing the password over the telephone upon confirmation that the email has been delivered.

4.4 The transmission of confidential information via e-mail to unauthorised persons is strictly prohibited.

4.5 All members of staff must ensure that confidential emails are not opened whilst their workstation/laptop or mobile device is connected to a projector.

4.6 When sending emails to a distribution group staff must ensure they select the correct distribution group for email delivery instead of sending emails to the All Staff Group. Group emailsshould only be sent to targeted individuals.

4.7 While the Advance Learning Partnership respects the privacy of staff, where there is reasonfor concern, the ALP reserves the right to monitor and intercept e-mail communication.

4.8 Members of staff should only open attachments to emails if they have come from someonethey know and trust. Attachments can contain viruses and other programs that could seriously damage the school ICT infrastructure. Any emails that seem suspicious must be brought to the attention of the Network manager for investigation.

4.9 Users who receive unsolicited mail should inform the network manager.

4.10 Members of staff must not send chain email or unsolicited commercial e-mail (also known as SPAM).

4.11 Any e-mail communication made must not bring the ALP into disrepute; this includes anything libellous, defamatory or criminal.

5. Printing

5.1 Staff should ensure that any documents printed use the correct admin code, if you believe youdo not have access to the correct department codes then please speak to a member of the IT support team.

5.2 Where possible staff should ensure documents are printed doubled sides and only in colour if required. The cost of printing colour documents will be charged at a higher rate.

5.3 Members of staff must also ensure that large volume photocopying (for an example a class setof resources) is passed through the reprographics department.

5.4 Heads of department will be issued each month with a staff break down of photocopying / print costs to allow middle leaders to track and encourage the use of reprographics and / or printing when necessary.

6. Shared Network Drive (Student Data / Staff Data)

6.1 All members of staff are provided with access to shared folders to enable the sharing of datato promote collaborative working. Each department is responsible for managing and maintainingits shared folder.

6.2 No personal or sensitive pupil data should ever be stored within the Student Shared Area (student data drive) unless appropriate security permissions have been applied to the containerfolder. As a guide only data to which pupils need access should be stored within the Student Shared Area.

6.3 Under no circumstances should anything which could be deemed as inappropriate (including potentially offensive, unsuitable or copyright infringing data) be stored in any of these areas. Any inappropriate content found within the shared areas will be reported to the network manager and the content deleted.

6.4 Staff should ensure that data stored on shared network drives such as student data and staffdata should be appropriate and remove files when no longer necessary in order to maximise storage capacity / network efficiency.

7. Portable Storage Encryption

It is a legal requirement of the GDPR (Data Protection) to protect and secure personal and sensitive data. The Information Commissioner's Office (ICO) recommends that portable and mobile devices (including media) used to store and transmit personal information, the loss of which could cause

damage or distress to individuals, should be protected using approved password techniques / encryption software which is designed to guard against the compromise of information.

7.1 Sensitive or personal information refers to any data that is protected by ALP policy, or by any local, or national laws or regulations. This includes but is not limited to:

i. Education records
ii. Employee records
iii. Personally identifiable information
iv. Confidential internal school information

7.2 Members of staff must not store any sensitive or personal information about staff, students or the school on any portable storage system unless that storage system is encrypted, password protected and approved for such use by the school. In such cases members of staff must contactthe ICT Support and Development Team to either be provided with an encrypted USB device or to have an existing storage system encrypted.

7.3 Storing sensitive or personal data on a USB device that is not protected from unauthorised access with encryption is a severe breach of this Acceptable Use Policy and the GDPR.

7.4 To ensure compliance with this policy and the GDPR the school reserves the right to monitor staff utilisation of USB devices used on the school network. Any breaches will be reported to theSenior Leadership Team and possible the ICO and other action, as appropriate taken.

7.5 Where possible staff wishing to access sensitive student data outside of school should make use of the remote access facility found on the school's website.

8 Electrical Equipment

8.1 Any mains operated personal computer or electrical equipment used on site, for any use, is subject to a Portable Appliance Test (PAT) by either site maintenance staff or a third party.

8.2 Members of staff must not connect any electrical equipment that has not been tested, unless the equipment is brand new or less than 12 months old.

8.3 Any electrical equipment with a damaged, frayed or exposed power cable must not be used. The damaged must be reported to site maintenance staff.

9 Additional Systems

9.1 Members of staff may have access to additional systems which include, but are not limited to SIMS, Arbor, SENSO, Impero, Classcharts, CPOMS, SISRA, Finance Software, the Durham Learning Gateway, Exam Software and Office 365.

9.2 These systems require additional passwords. It is the responsibility of the member of staff toensure that their password has basic complexity to it and that they only know their password. A password with basic complexity is one that is at least 8 characters in length and uses a combination of upper, and lower case letters, numbers and symbols.

10 ICT Equipment and Suites

10.1Staff should not move or authorise any person to move any ICT Equipment located within the school or any ICT Suites unless as part of authorised work/repair.

10.2Staff may not pass on any ICT Equipment to any other person. It must first be passed back to the IT support team so that it can be reissued

10.3 Any equipment issued to staff remains property of the school and must be returned upon request. The issued equipment must also be available for inspection at all reasonable times

10.4 If a mobile device is provided it is expected that the device should be brought to school on a daily basis.

10.5 Upon termination of employment at the school all equipment must be returned, failure to do so may fail in payment for the device.

10.6 Staff are responsible for all equipment issued to them and must take reasonable precautions to protect such equipment.

10.7 Staff are responsible for all equipment and use of workstations and laptops by students during their lessons. Individual departments will be billed for any associated damage.

10.8 Shared devices such as iPads must be booked using the online booking system before use.

10.9 Staff must ensure that students do not consume any food or drink whilst working on any ICT equipment.

10.10 All available ICT Suites must be booked using the online booking system before use.

10.11 Staff must ensure that ICT Suites are locked upon leaving the room. Students should not be allowed access to keys to ICT Suites at any time.

10.12 No students should be allowed to use ICT Suites without supervision by a member of staff.

10.13 Students are only allowed to use workstations/laptops that have been configured for student use. Under no circumstances must a student be allowed to log on to a workstation/laptop issued toa member of staff. Allowing a student to do so constitutes a breach of this policy.

10.14 Before purchasing any hardware or software members of staff should consult a member of the IT Support Team to check compatibility, license compliance and discuss any other implicationsthat the purchase may have.

11 Creation, Distribution & Publication of Digital Media

11.1 Members of staff will always use school owned equipment for taking images and recording videos of pupils.

11.2 The use of any personal device to photograph or video school students is only permissible following application to the Headteacher.

11.3 Any digital images taken should be transferred and deleted as soon as is reasonably possible. Retaining digital media of students on any personal device owned by staff is a serious breach of thisAcceptable Use Policy and any instances of this will be reported to the Senior Leadership Team andappropriate action taken.

11.4 Unless digital media of students is required by an external agency for professional printing or external publication photographs and videos of students will not be distributed unnecessarily.

11.5 All media published online and media sent to external agencies requires the approval of the school Senior Leadership Team.

11.6 Members of staff must ensure that parental permission has been obtained before any students are photographed or filmed whilst at school or taking part in a school activity.

12 Reporting Problems

12.1 Problems that seriously hinder your job or teaching and require immediate attention should be reported by telephone or in person to the IT support team as well as logging on Every Compliance system. All other problem must be reported via the helpdesk located in the shortcuts folder on staffdesktops that all members of staff have access to.

12.2 Data loss should be reported to the ICT Support and Development Team as soon as possible. The longer a data loss problem goes unreported, the less the chances of the data being recovered.

13 Internet Access

13.1 The use of the Internet for personal purposes is permitted but must be limited to before/after school, during designated break periods and lunch time only.

13.2 All Internet access is logged for the purposes of maintaining standards of security andacceptable use.

13.3 This Acceptable Use Policy covers Internet access by staff using school devices as well as personal devices if the personal device is connected to the school network.

13.4 Attempts to access inappropriate websites, websites which attempt to bypass filtering systems or personal use of the Internet outside of the designated times constitutes a breach of this Acceptable Use Policy.

13.5 Inappropriate websites referred to in 13.4 include, but are not limited to any site whichcontains:

- Pornographic Material (of either a legal or illegal nature).
- Material which incites hatred or discrimination.
- Material which promotes illegal activity.
- Material which is in breach of the GDPR.
- Material which is degrading to persons or groups of persons.

13.6 Staff are required to report any websites that they become aware of, which are not filteredand that are deemed inappropriate as per the criteria stated within 13.5.

13.7 While the ALP respects the privacy of its staff, where there is reason for concern, the ALP reserves the right to perform a detailed audit of all network activity.

13.8 Reason for concern referred to in 13.7 include, but are not limited to the following:

- A complaint made by a student
- A complaint made by a visitor to the school
- A complaint made by a parent/carer

13.9 A detailed audit of network activity can only be requested by a member of the Senior Leadership Team. The request must be made in writing and must be accompanied by documentaryevidence supporting the request.

13.10 While the Advance Learning Partnership uses sophisticated filtering technology and takes all precautions to ensure that users only access appropriate material, it is not possible to guarantee that unsuitable material will be inaccessible. The ALP cannot accept liability for the material accessed, or any consequences of such access.

14 Social Media/Mobile

Please refer to the Online Safety Policy regarding social media and use of mobile phones.

Guidance about safeguarding staff on social media:

It is important that staff that are approached by pupils on social media do not "friend" them and that if the young person is under the age required by that service this information is passed to either the e-safety or safeguarding lead. Staff should screenshot any pupil friend requests so that it is clear who has made the friend request in the event of an allegation against a member of staff. Any allegation made against a member of staff will need to be investigated and may be referred to the Local Authority Designated Officer (LADO).

15 GDPR and Freedom of Information

15.1 All information about staff will be dealt with in compliance the GDPR and only given to authorised agencies.

15.2 Under the Freedom of Information Act 2000 all members of staff have the right to request information held on the school system regarding their network activity. Staff wishing to request suchinformation will need to complete an Information Request form.

16 Legislation

16.1 All network users are bound by current relevant legislation. The applicable laws (as amended)

include, but are not limited to:

- Computer Misuse Act 1990
- Copyright Designs and Patents Act 1998
- Criminal Justice Act 1988
- Defamation Acts 1952 and 1996
- Freedom of Information Act 2000
- Human Rights Act 1998
- Obscene Publications Act 1959 and 1964
- Protection of Children Act 1988
- Protection from Harassment Act 1997
- Public Order Act 1986
- Race Relations Amendment Act 2000
- Telecommunications Act 1984
- GDPR 2018
- Sex Discrimination Act 1986
- Regulation of Investigatory Powers Act (RIPA) 2000
- Online Safety Act 2023

16.2 Staff should understand that any attempt to bypass the school, or other network security systems, including the introduction of viruses or applications of a destructive nature could lead to prosecution.

16.3 Where it is believed that a member of staff is in breach of legislation appropriate action willbe taken.

17 Reporting Breaches of this Policy

17.1 All members of staff have a duty to ensure this Acceptable Use Policy is followed. You must immediately inform a member of the ICT Support and Development Team and the Senior Leadership Team of any breaches.

17.2 Members of staff are required to report:

- Inappropriate content suspected to be stored on the computer system.
- Websites accessible from within school unsuitable for staff or student consumption;
- Breaches, or attempted breaches, of computer security.
- Any instance of bullying or harassment via the school computer system.

18 Sanctions

In the event that this Acceptable Use Policy is breached, staff will be subject to sanctions which may include, but are not limited to:

- Disciplinary procedures
- Temporary or permanent restriction of network access or network rights
- Restriction to or denial of access to ICT Suites
- Investigation under the Regulation of Investigatory Powers Act (RIPA) 2000

Staff Agreement

I have read and understood the Staff Acceptable Use Policy for the Advance Learning Partnership.

I understand that should I be found in breach of the Acceptable Use Policy I may be liable to disciplinary procedures and, if appropriate, the Police and local authorities may become involved.
I accept that it is my responsibility to be aware of amendments to this Acceptable Use Policy, via the Policy Management System.

Appendix 2. – Laptop/Device Loan Scheme – Pupils

Get help with Technology programme

We are loaning you this laptop/device for the benefit of your child in supporting and developing their education. With this computer your child will be able to build on and enhance their skills, knowledge and understanding.

1. The loan agreement exists between the school and the Named Person who has signed this loan agreement.

Pupil Name: _____

Parent/Carers Name & Address:_____

2. The laptop/device will be loaned to the named person for the duration of the period in which the child within their care is on the roll,

Device Model: _____

Device Serial Number: _____

When it is time to return the device/laptop the device/laptop must be returned to the academy in full working order and in good condition including all accessories, no later than the_____.

3. Should you move address from the location you have given us, it is essential that you inform your school at the earliest opportunity.

4. You will be issued with a laptop/device and power supply. These remain the property of the school.

5. You will be able to install licensed legally purchased software and equipment such as printers and scanners on your computer. At no point must you open the computer and make changes to the inner hardware.

6. The laptop/device and the connectivity equipment must not be used for any illegal and/or antisocial purpose.

7. There may be occasions when we need you to return the computer to school for upgrades and maintenance. Please note that because of these upgrades, it may be necessary to completely remove all information contained on the computer. The school cannot be held responsible for the loss or damage of any data on the computer during this process. It is your responsibility to return the computer to school.

During this process, technical members of staff may view data or programmes on the computer. You will be held responsible to the acceptable use policy at this point. You may want to remove personal data from the computer before its return.

8. All technical support and maintenance must go through the school.

9. If your computer is stolen you must immediately report it to the police and get a crime reference number. Immediately report this to us; we will make every effort to replace the computer when we are able.

10. If your computer is accidentally damaged, immediately contact us. We will do our best to repair the damage, if this is not possible, replacement will be on a case by case basis.

Any malicious damage to the device or accessories will be chargeable.

Responsibilities you have to care for your laptop/device

11. You have a responsibility to take reasonable care to ensure the security of the computer and connectivity equipment.

12. You must not decorate or change the external face of the equipment provided in any way, including affixing stickers.

13. Reasonable health and safety precautions should be taken when using a computer. The school is not responsible for any damage to person or property resulting from the computer or equipment loaned.

14. The school is not responsible for any costs resulting from the use of the computer and the connectivity equipment, including electricity, printer cartridges, paper or any cost occurring from an Internet service not provided by the school.

I, the parent/carer, have read or had explained and understand the terms and conditions in the Get help with technology programme. I understand that by breaching the conditions the loan of the computer may be withdrawn by the school.

Signed_____Date_____

Printed Name _____

School Address:

Appendix 3. – Student Acceptable Use Policy

Student Name: Tutor Group:

Policy Overview

The Advance Learning Partnership has provided computers and other resources to students in order to help support them with the curriculum. If access to these devices and resources is misused, then access maybe withdrawn. The academies of the Advance Learning Partnership encourage students to make use of these facilities for their benefit and to use them safely and responsibly.

ICT Equipment

- Students are not allowed to access ICT resources unless supervised by a member of staff.
- Damaging, disabling or otherwise harming the operation of computers is not permitted.
- All computer systems use must be appropriate to the student's education.

Security and Privacy

- Computer access must only be made via the students own authorised account and password. This must not be used by any other person.
- Passwords must be secure and changed regularly to protect their account.
- Any attempt to bypass the schools' security systems may result in disciplinary action or prosecution.
- The school will exercise its right to monitor the use of the computers systems.

Removable Storage Devices / Online Storage

- Removable storage devices such as USB memory sticks or the Cloud, must be checked with antivirus software and only be used if they have been found to be clear of viruses.
- Files within computer storage areas / removable storage may be monitored to ensure no inappropriate content is being stored or brought into school.

Internet Access

- All Internet activity is logged by the schools web filtering software and is reviewed on a regular basis.
- Access to the Internet is for study or for school authorised activities only.
- Only access to suitable materials online is allowed. Using the Internet to download, send, print, display or otherwise gain access to materials that are unlawful, obscene or abusive is not permitted.
- Social networking websites and messaging facilities are not permitted.

Electronic Mail

- All e-mail activity is monitored, tracked and logged.
- Attachments should only be opened if the source is known and trusted.
- Any emails that contain violent, racist or inappropriate content should be reported to a member of staff.

Printing

- All printing activity is monitored and logged.
- Work should only be printed when instructed to do so by a member of staff. Personal printing is not permitted.

I/we agree to my child using the school's ICT facilities under the conditions above.
I/we agree that if my child misuse the ICT equipment, this may result in its use being withdrawn in school. This may also result in further disciplinary action and / or prosecution.

I/ we will support the schools approach to online safety and not deliberate post comments or upload images, sounds or message that could upset of offend any member of the school community or bring the school into disrepute.

Signed: …… (student) Date: ……

Signed: …… (parent/carer) Date: ……