Online Safety Policy

146-148 Park View Road
Welling
Greater London
DA16 1SR

The School's electronic communications systems and equipment are intended to promote effective communication and working practices throughout the business and are critical to the success of our provision of excellent service.

This policy does not form part of any employee's terms and conditions of employment and is not intended to have contractual effect. It is provided for guidance to all members of staff at the School who are required to familiarise themselves and comply with its contents. The School reserves the right to amend its content at any time.

This policy outlines the standards that the School requires all users of these systems to observe, the circumstances in which the School will monitor use of these systems and the action the School will take in respect of any breaches of these standards.

This policy is to be read in conjunction with the following policies:

Monitoring
Social Media
Security
Code of Conduct
CCTV

The use by staff and monitoring by the School of its electronic communications systems is likely to involve the processing of personal data and is therefore regulated by the Data Protection Act 2018, together with the Employment Practices Data Protection Code issued by the Information Commissioner.

Staff are referred to the School's Data Protection Policy for further information. The School is also required to comply with the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and the principles of the European Convention on Human Rights incorporated into U.K. law by the Human Rights Act 1998.

All members of staff are required to comply with the provisions set out in this policy at all times to protect the School's electronic systems from unauthorised access or harm. Breach of this policy will be regarded as a disciplinary offence and dealt with under the School's disciplinary procedure and in serious cases may be treated as gross misconduct leading to summary dismissal.

The School has the right to monitor all aspects of its systems, including data which is stored under the School's computer systems in compliance with the Data Protection Act 2018.

This policy mainly deals with the use (or misuse) of computer equipment, e-mail, internet connection, telephones, iPads (and other mobile device

tablets), Blackberries, personal digital assistants (PDAs) and voicemail, but it applies equally to the use of fax machines, copiers, scanners, and the like.

Equipment Security and passwords

All members of staff are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this policy.

Passwords are unique to each user and must be changed regularly to ensure confidentiality. Staff are required to select a password that cannot be easily broken and which contains at least 8 characters including both numbers and letters.

Passwords must be kept confidential and must not be made available to anyone else unless authorised by a member of the Senior Leadership Group who will liaise with the IT Department as appropriate and necessary. Any member of staff who discloses his or her password to another employee in the absence of express authorisation will be liable to disciplinary action under the School's Disciplinary Policy and Procedure. Any member of staff who logs on to a computer using another member of staff's password will be liable to disciplinary action up to and including summary dismissal for gross misconduct.

If given access to the School e-mail system or to the internet, staff are responsible for the security of their terminals. Staff are required to log off when they are leaving the terminal unattended or when leaving the office to prevent unauthorised users accessing the system in their absence. The Senior Leadership Group and/or IT Department may do spot checks from time to time to ensure compliance with this requirement.

Staff should be aware that if they fail to log off and leave their terminals unattended they may be held responsible for another user's activities on their terminal in breach of this policy, the School's Data Protection Policy and/or the requirement for confidentiality in respect of certain information.

Logging off prevents another member of staff accessing the system in the user's absence and may help demonstrate in the event of a breach in the user's absence that he or she was not the party responsible.

Staff without authorisation should only be allowed to use terminals under supervision. Desktop PCs and cabling for telephones or computer equipment should not be moved or tampered with without first consulting and obtaining the express approval of the IT Department.

On the termination of employment for any reason, staff are required to provide a full handover detailing the drives, folders and files where their work can be located and accessed and sign out of school accounts on all devices. The

School reserves the right to require employees to hand over all School data held in computer usable format.

Members of staff who have been issued with a laptop, Mobile Tablet (Ipad), mobile phone or VOIP Phone must ensure that it is kept secure at all times, especially when travelling. Passwords must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event that the machine is lost or stolen. Staff should also observe basic safety rules when using such equipment e.g. ensuring that they do not use or display such equipment in isolated or dangerous areas. Staff should also be fully aware that if using equipment on public transport documents can be easily read by other passengers.

Systems Use and Data Security

Members of staff should not delete, destroy or modify any of the School's existing systems, programs, information or data which could have the effect of harming or exposing to risk or harm the School's, its staff, students, or any other party.

All members of staff are prohibited from downloading, installing or running software from external sources without obtaining prior authorisation from the IT Department who will consider bona fide requests for work purposes. Please note that this includes instant messaging programs, screensavers, photos, video clips, games, music files and opening any documents or communications from unknown origins.

All Members of Staff can freely access the chrome web store and add any app or extension they wish providing it is inline with the policies set out. The school has taken the steps to become a Google technology based establishment and will provide all users a chrome based computer if they are required to have one. All safety and security settings are automatically pushed out to all users to prevent unauthorised access to harmful sources.

For security purposes the company does not allow users to bring their own devices onto the network this includes Mobile Phones, Computers and Tablets (ipads), all user owned devices are not covered by the company's insurance policies for any damage that may occur. Any user that requires constant access to a device should contact their Manager for authorisation.

Only school owned chrome devices are permitted to be used for work purposes, personal chrome devices do not get the security measures pushed out to them due to the enrollment process.

Where consent is given all files and data should always be virus checked before they are downloaded onto the School's systems. If in doubt, the employee

should seek advice from the IT Department or a member of the Senior Leadership Group.

The following must never be accessed from the network because of their potential to overload the system or to introduce viruses:

- audio and video streaming;
- instant messaging;
- chat rooms;
- social networking sites; and
- Personal web mail (such as Gmail,Hotmail or Yahoo).

With the exception of use for the benefit of work (such as Google meet to contact for remote working), and access to School managed social media platforms where permission has been granted by the SLT and IT Department.

No device or equipment should be attached to our systems without the prior approval of the IT Department. This includes, but is not limited to, any PDA or telephone, iPad (or other mobile device tablet), USB device, i-pod, digital camera, MP3 player, infrared connection device or any other device.

The School monitors all emails passing through its systems for viruses. Staff should be cautious when opening emails from unknown external sources or where for any reason an email appears suspicious (such as ending in '.exe'). The IT Department should be informed immediately if a suspected virus is received.

The School reserves the right to block access to attachments to email for the purpose of effective use of the system and compliance with this policy. The Schools systems keep a secure record of all messaging, email and browsing data of every user, which the IT department can access at any time without permission in the interest of safeguarding and may be required to pass this information on to relevant authorities if asked to. The School also reserves the right not to transmit any email message.

Staff should not attempt to gain access to restricted areas of the network or to any password-protected information unless they are specifically authorised to do so.

Misuse of the School's computer systems may result in disciplinary action up to and including summary dismissal. For further guidance on what constitutes misuse please see the section entitled Inappropriate Use of the School's Systems and guidance under "E-mail etiquette and content" below.

E-mail etiquette and content

E-mail is a vital business tool, but often lapses inappropriately into an informal means of communication and should therefore be used with great care and discipline.

The School's email and phone facility is intended to promote effective communication within the business on matters relating to the School's business activities and access to the School's email and phone facility is provided for work purposes only.

Staff are strictly prohibited from using the School's email facility for personal emails at any time.

Staff are strictly prohibited from adding their school email onto their personal phone unless instructed otherwise by a member of the SLT or they are a member of the SMT and have authorisation from the IT Department to do so.

Staff should always consider if email is the appropriate medium for a particular communication. The School encourages all members of staff to make direct contact with individuals rather than communicate by email wherever possible to maintain and enhance good working relationships.

Messages sent on the email system should be written as professionally as a letter or fax message and should be concise and directed only to relevant individuals on a need to know basis. The content and language used in the message must be consistent with the School's best practice.

Emails should never be sent in the heat of the moment or without first checking the content and language and considering how the message is likely to be received. Staff are encouraged wherever practicable to write a draft email first, review it carefully or send to another member of staff before finalising and sending. As a rule of thumb if a member of staff would not be happy for the email to be read out in public or subjected to scrutiny then it should not be sent. Copies of all emails are retained securely on the schools G suite system.

All members of staff should remember that emails can be the subject of legal action for example in claims for breach of contract, confidentiality, defamation, discrimination, harassment etc against both the member of staff who sent them and the School. Staff should take care with the content of email messages, as incorrect or improper statements can give rise to personal liability of staff and to liability of the School in the same way as the contents of letters or faxes.

Email messages may of course be disclosed in legal proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an email is obliterated and all email messages are retrievable, either

from the main server or using specialist software. This should be borne in mind when considering whether e-mail is an appropriate forum of communication in the circumstances of the case and if so the content and language used.

Staff should assume that e-mail messages may be read by others including any person mentioned or otherwise identified in the content of the email and not include in them anything which would offend or embarrass any reader, or themselves, if it found its way into the public domain. The School standard disclaimer should always be used on every email.

Staff should ensure that they access their emails at least once every Contracted working day, stay in touch by remote access when travelling or working out of the office and should use an out of office response when away from the office for more than a day. Staff should endeavour to respond to emails marked 'high priority' as soon as is reasonably practicable.

Members of staff are strictly forbidden from sending abusive, obscene, discriminatory, racist, harassing, derogatory or defamatory messages. If such messages are received, they should not be forwarded or responded to and should be reported to a member of the Senior Leadership Group immediately. If a recipient asks you to stop sending them personal messages then always stop immediately. Where appropriate, the sender of the email should be referred to this policy and asked to stop sending such material.

If you feel that you have been harassed or bullied, or are offended by material sent to you by a colleague via email, you should inform your Line manager/Head of Department or the Headteacher who will usually seek to resolve the matter informally. You should refer to our Equal Opportunities and Dignity at work/Bullying Policy for further information and guidance.

If an informal procedure is unsuccessful, you may pursue the matter formally under the School's formal grievance procedure. (Further information is contained in the School's Equalities Policy, Anti-Harassment and Bullying Policy and Grievance Policy and Procedure.)

As general guidance, staff must not

Send any email, including resending and forwarding, containing sexually explicit or otherwise offensive material either internally or externally;

- Send any e-mail communication which may be regarded as harassing or insulting. Complaints about the performance or service of other departments or individuals must be made on a face-to-face basis in accordance with normal and courteous practice;
- Send or forward private emails at work which they would not want a third party to read;
- Send or forward chain mail, junk mail, cartoons, jokes or gossip either within or outside the School;

- Contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding emails to those who do not have a real need to receive them;
- Sell or advertise using the systems or broadcast messages about lost property, sponsorship or charitable appeals.
- Agree to terms, enter into contractual commitments or make representations by e-mail unless the appropriate authority has been obtained. A name typed at the end of an e-mail is a signature in the same way as a name written in ink at the end of a letter;
- Download or email text, music and other content on the internet subject to copyright protection, unless it is clear that the owner of such works allows this;
- Send messages containing any reference to other individuals or any other business that may be construed as libellous;
- Send messages from another worker's computer or under an assumed name unless specifically authorised;
- Send confidential messages via e-mail or the internet, or by other means of external communication which are known not to be secure;
- E-mail may normally only be used to communicate internally with colleagues and students (where appropriate and necessary) and externally to parents, suppliers and third parties on academic/service related issues. Urgent or important messages to family and friends are permitted, but must be of a serious nature;
- Allow any learner access to your ID card/door entry card. Losses mauy need to be paid for.

The School recognises that it is not always possible to control incoming mail. Any material which would be considered as inappropriate or unprofessional, sexually explicit or offensive should be deleted at once. Any member of staff who finds that they are receiving such communications from known sources is responsible for contacting that source in order to request that such communication is not repeated and contacting the IT Department for further action to be taken to prevent future issues to other users.

Staff who receive an email which has been wrongly delivered should return it to the sender of the message. If the email contains confidential information or inappropriate material (as described above) it should not be disclosed or forwarded to another member of staff or used in any way unless being sent to the IT Department for actioning at their request. Your Line Manager/Head of Department or the Headteacher should be informed as soon as reasonably practicable.

Use of the web and the internet

When a website is visited, devices such as cookies, tags or web beacons may be employed to enable the site owner to identify and monitor visitors. If the website is an inappropriate one such a marker could be a source of embarrassment to the School, especially if a member of staff has accessed,

downloaded, stored or forwarded inappropriate material from the website. Staff may even be committing a criminal offence if, for example, the material is pornographic in nature, Any inappropriate website should be brought to the immediate attention of the IT Department.

Staff must not therefore access from the School's system any web page or any files (whether documents, images or other) downloaded from the web which, on the widest meaning of those terms, could be regarded as illegal, offensive, in bad taste or immoral. While content may be legal in the UK it may be in sufficient bad taste to fall within this prohibition.

As a general rule, if any person within the School (whether intending to view the page or not) might be offended by the contents of a page, or if the fact that the School's software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy, if school installed software does access such a page this the IT Department and SLT should be made aware of this as soon as possible.

Staff should not under any circumstances use School systems to participate in any internet chat room, post messages on any internet message board or set up or log text or information even in their own time.

Remember also that text, music and other content on the internet are copyright works. Staff should not download or e-mail such content to others unless certain that the owner of such works allows this.

The School's website may be found at http://alpschools.org/. This website is intended to convey our core values and excellence in the educational sector. All members of staff are encouraged to give feedback concerning the site and new ideas and inclusions are welcome. All such input should be submitted to the Senior Leadership Group in the first instance. Only expressly authorised and designated members of staff are permitted to make changes to the website.

The School has published relevant information on its own intranet for the use of all staff. All such information is regarded as confidential to the School and may not be reproduced electronically or otherwise for the purposes of passing it to any individual not directly employed by the School. Any exceptions to this must be authorised by Human Resources who will liaise with the Senior Leadership Group as appropriate and necessary.

Personal use of the School's systems

Staff are strictly prohibited from personal use of the School's systems.

Staff should be aware that any personal use of the systems may also be monitored (see below) and, where breaches of this policy are found, action may be taken under our Disciplinary Policy and Procedure. Any personal use of

the School's email facility will be treated as a disciplinary offence resulting in disciplinary action up to and including summary dismissal depending on the seriousness of the offence.

The School reserves the right to restrict or prevent access to certain telephone numbers or internet sites if it considers that personal use is excessive or otherwise in breach of this policy.

Mobile Equipment

This policy covers the use of laptops and mobile devices and phones. If provided by ASD Learning Ltd it also covers the allocation of these devices, and their use by employees. Where provided by ASD Learning Ltd., these devices represent a significant expense and it is important that you are familiar with this policy. Failure to comply with this policy could result in action under the School's Disciplinary Policy. All mobile devices provided to the employee by ASD Learning Ltd. are to be returned to the School on termination of employment.

Care of Equipment

Mobile equipment users will be responsible for taking reasonable care of their equipment and associated accessories. Be wary of common scams at airport security checkpoints and other public places. Avoid leaving your equipment in a car, but if you have to, place it in the boot ***prior to your arrival*** and ensure that the boot is locked. The School's insurance will not pay out for equipment stolen from a car which was not locked in the boot.

ASD Learning Ltd may remove your right to use a School mobile device if it is abused. School equipment should not be lent to anyone else (including family members).

Usage of School Mobile Equipment

All School phone bills will be monitored and excessive usage may require justification. ASD Learning Ltd allocates mobile equipment to certain members of staff as business tools to help them to perform their jobs effectively and they should be used primarily for business work.

The School accepts that employees may make some private use of mobile telephones but you are requested to keep this to a minimum – this also applies to text messaging and data. See mobile phone usage policy below. School mobile phones should only be used to make calls to premium rate numbers where the nature of the call relates to School business. You should be aware that roaming charges when abroad may be very high and you should bear this in mind when making and receiving calls or using data. Unless required for urgent business matters, data roaming should be turned off and free wireless networks used as an alternative.

You must not use a hand held mobile telephone while driving. You may only use a hands-free on a School mobile telephone when it is safe to do so and you must comply at all times with all applicable legal requirements including the Highway Code. See the driving at work policy for more information on this.

You must not use a School mobile telephone for any illegal or immoral activity.

Loss or Damage of Mobile Equipment

The loss or theft of a School mobile device must be reported immediately to the IT department or a member of the SMT.

Stolen/lost mobile devices should also be reported to the Police and a Police statement supplied for insurance purposes. A crime report number will ensure a FOC replacement. Unjustified delay or failure to report the loss or theft of a mobile phone could result in subsequent call charges being re-charged to the employee.

Stolen/lost mobile devices will be replaced with the current model of device. You may be held responsible at the School's discretion for the cost of the replacement unit and SIM card if the loss or theft results from your negligence or from a clear failure to comply with this policy.

Damaged devices that can be repaired will be repaired. You may be held responsible at the discretion of the School for the cost of the repairs, where the damage results from your negligence or from a clear failure to comply with this policy.

ASD Learning Ltd reserves the right to monitor School mobile devices, both during routine audits and in specific cases where a problem relating to excessive or unauthorised use is suspected. The purposes of such monitoring include checking that the use of ASD Learning Ltd.'s mobile equipment is not being abused or used in an unauthorised manner, ensuring there is no unauthorised use of ASD Learning Ltd's time and ensuring that inappropriate websites are not being accessed from School mobile devices. Therefore, in relation to School mobile phones, ASD Learning Ltd reserves the right to obtain an itemised list from the mobile phone service provider of all outgoing calls made on the mobile phone.

This list may include details of each number called, the date, time and duration of each call and the cost of each call. In addition, ASD Learning Ltd reserves the right to obtain an itemised list from the mobile phone service provider of all outgoing text messages sent from the mobile phone. This list may include details of each number texted, the date and time of each text message and the cost of each text message.

Where exceptional circumstances warrant it, ASD Learning Ltd may also ask the mobile phone service provider to provide access to the actual content of text messages.

Finally, where applicable, ASD Learning Ltd may request Internet access records from the mobile phone service provider, including websites visited and the amount of mobile data used.

For more details on monitoring of mobile devices please refer to the monitoring policy.

Mobile Equipment Usage on ASD Learning Ltd Premises

Aims of this Policy

- To inform employees about our policy within the workplace.
- To protect employees from danger caused by distraction.
- To uphold standards of quality.

Essential Elements

- Whilst the School will tolerate the use of mobile phones for essential personal calls during normal working hours at the agreement of the SMT, excessive use for personal calls is prohibited.
- Also prohibited are lengthy calls, casual chats, text messaging, e-mailing, web browsing and the taking of video and/or still images (if your phone is so enabled).
- If you have a School-issued mobile phone, you are not to take any pictures/video on it that you would not be happy your Line Manager seeing.
- **Your private mobile phone should be set to a silent ring during normal working hours.**
- **Personal use of your mobile phone should be done outside your normal working hours or during set break periods unless otherwise agreed with the SMT**.
- **Do not bring in electrical items to your workplace unless absolutely necessary.**
- **Use of mobile phones for work purposes is considered acceptable.**
- **Do not allow any learner to have access to your ID card/door entry card.**
- **Any lost ID cards may have to be paid for to replace.**
- **Report any lost equipment as soon as possible.**

For mobile phones and driving see the Driving at work policy.

Inappropriate use of equipment and systems

Access is granted to the web, telephones and to other electronic systems, for legitimate work purposes only.

Misuse or abuse of our telephone or e-mail system or inappropriate use of the internet in breach of this policy will be dealt with in accordance with the School's Disciplinary Policy and Procedure.

Misuse of the internet may, in certain circumstances, constitute a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet by viewing, accessing, transmitting or downloading any of the following material, or using any of the following facilities, will amount to gross misconduct (this list is not exhaustive):

(a) Accessing pornographic material (that is writings, pictures, films, video clips of a sexually explicit or arousing nature), racist or other inappropriate or unlawful materials;
(b) Transmitting a false and/or defamatory statement about any person or organisation;
(c) Sending, receiving, downloading, displaying or disseminating material which is discriminatory, offensive, derogatory or may cause offence and embarrassment or harass others;
(d) Transmitting confidential information about the School and any of its staff, students or associated third parties;
(e) Transmitting any other statement which is likely to create any liability (whether criminal or civil, and whether for the employee or for the School;
(f) Downloading or disseminating material in breach of copyright;
(g) Copying, downloading, storing or running any software without the express prior authorisation of IT Department;
(h) Engaging in online chat rooms, instant messaging, social networking sites and online gambling;
(i) Forwarding electronic chain letters and other materials;
(j) Accessing, downloading, storing, transmitting or running any material that presents or could present a risk of harm to a child.

Any such action will be treated very seriously and may result in disciplinary action up to and including summary dismissal.

Where evidence of misuse is found the School may undertake a more detailed investigation in accordance with our Disciplinary Policy and Procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or members of management involved in the disciplinary procedure.

If necessary such information may be handed to the police in connection with a criminal investigation.

VOIP Phones

The Voice Over Internet Protocol phones or VOIP phones are directly connected to the internet and a remote support company currently ensures the network

runs as it should which includes the internet the computers use. If you ever have any drops in calls or problems with the VOIP phones or network on the computer you are using contact the I.T. department immediately to ensure and issues are resolved in good time.

There is a universal contact sheet that can be found on Staffnet. These numbers are for internal use only and would not work from any other phone. External calls should go to the main incoming number which is: 0203 137 3630 and callers are then directed with the use of a voice over menu system.

I.T. Support Contacts:
For all General IT Related Queries please use the Ticket system or send an email to tech-support@alpschools.org

IT Manager
Graham Gosden
Email: graham.gosden@alpschools.org
Internal Ext. 1001

IT Administrator
Tom Henderson
Email: tom.henderson@alpschools.org
Internal Ext. 1002

Local IT Support (South East)
Brandon Hygate
Email: brandon.hygate@alpschools.org
Internal Ext. 1055

Local IT Support (Midlands)
Kyle Spencer
Email: kyle.spencer@alpschools.org
Internal Ext. 1156