



ALDERLEY EDGE
SCHOOL FOR GIRLS

CYBER and ONLINE SAFETY POLICY WHOLE SCHOOL & EYFS

Reviewed: Autumn 2024
Governor Review: Autumn 2024

CONTENTS

Development, monitoring and review of the Policy	3
Schedule for development, monitoring and review	3
Scope of the Policy	3
Roles and Responsibilities	4
• Governors	4
• Headteacher and SLT	4
• Online Safety Online safety Officer	4
• IT Development Manager / Technical Staff	5
• Teaching and Support Staff	5
• Child Protection / Safeguarding Designated Person / Officer	5
• Online Safety Committee	6
• Pupils	6
• Parents	6
• Policy Statements	7
• Education – Pupils	7
• Education – Parents	8
• Education and training – Staff / Volunteers	8
• Training – Governors	8
• Technical – Cyber Security	8
• Technical – infrastructure / equipment, filtering and monitoring	9
• Bring your own devices (BYOD)	11
• Use of digital and video images	11
□ Youth Produced Sexual Images (YPSI, previously known as sexting)	12
• Data Protection	13

• Online Remote Learning During School Closure	13
• Communications	14
• Social Media - Protecting Professional Identity	15
• Responding to incidents of misuse	16

Appendices

• ICT Acceptable Use Policy Agreement - Pupils (Younger)	18
• ICT Acceptable Use Policy Agreement - Pupils (Older)	19
• ICT Acceptable Use Policy Agreement - Staff and volunteers	21
• BYOD Policy Agreement	24
• Use of digital and video images Policy	25
• Publication of Photographs and other forms of Media Consent Form	32
• Data Protection Policy	33
• School Technical Security Policy	35
• Internet Filtering Security	37
• Cyber Essentials IT Review	39
• Abuse of Staff Via Social Media	42
• Senior Pupil Agreement for Online Learning from Home	44
• Staff Agreement for Online Teaching from Home	46
• Prep School and EYFS Pupil Agreement for Online Learning from Home	50

Development / Monitoring / Review of this Policy

This online safety Online safety policy has been developed by a committee made up of:

- SLT
- Online Safety Officer / Coordinator
- Staff – including Teachers, Support Staff, Technical staff
- Governors
- Parents and Carers
- Students

This policy should also be read in conjunction with:

Schedule for Development / Monitoring / Review

This Online safety policy was approved by the Governing Body on:	TBC
The implementation of this Online safety policy will be monitored by the:	Online safety Deputy Head and IT Development Manager
Monitoring will take place at regular intervals:	In Online Safety Committee Meetings
The Online safety Policy will be reviewed every three years, or more regularly in the light of any significant new developments in the use of the technologies, new threats to Online safety or incidents that have taken place. The next anticipated review date will be:	May 2026
Should serious Online safety incidents take place, the following external persons / agencies should be informed:	PC Andrew Cornall / CEOP

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers / Principals 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 Online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for electronic

devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published **Behaviour Policy**.

The school will deal with such incidents within this policy and associated behaviour and antibullying policies and will, where known, inform parents of incidents of inappropriate Online safety behaviour that take place out of school. This policy should also be read in conjunction with the Staff Code of Conduct and the Child Protection & Safeguarding Policy.

Roles and Responsibilities

The following section outlines the Online safety roles and responsibilities of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the Online safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about Online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of online safety Governor. The role of the online safety Governor will include regular meetings with the Online Safety Committee

Headteacher and SLT:

- The Headteacher has a duty of care for ensuring the safety (including Online safety) of members of the school community, though the day to day responsibility for Online safety will be delegated to the Online safety Officer.
- The Headteacher and the Deputy Headteacher should be aware of the procedures to be followed in the event of a serious Online safety allegation being made against a member of staff.
- The Headteacher / SLT are responsible for ensuring that the Online safety Officer and other relevant staff receive suitable training to enable them to carry out their Online safety roles and to train other colleagues, as relevant.
- The Headteacher / SLT will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal Online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The SLT will receive regular monitoring reports from the Online safety Officer.

Online safety Officer:

- leads the Online safety committee
- takes day to day responsibility for Online safety issues and has a leading role in establishing and reviewing the school Online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an Online safety incident taking place.
- provides training and advice for staff
- liaises with the LA / relevant body
- liaises with school technical staff
- receives reports of Online safety incidents and creates a log of incidents to inform future Online safety developments
- meets regularly with Online safety Committee to discuss current issues, review incident logs and filtering / change control logs
- reports regularly to SLT

IT Development Manager / Technical staff:

The IT Development Manager is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required Online safety technical requirements
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- the filtering policy is applied and updated to all school devices and any BYOD devices on a regular basis and that its implementation is not the sole responsibility of any single person. Any changes to the filtering policy should be fully documented to provide a full audit trail.
- that they keep up to date with Online safety technical information in order to effectively carry out their Online safety role and to inform and update others as relevant
- that the use of the network / internet / cloud based services (such as MS Teams and the O365 suite) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher and Online safety Officer for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies
- that the Cyber Essentials certification is maintained on an annual basis.

Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of Online safety matters and of the current school Online safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy Agreement (AUP) and any amendments / updates issued during the lifetime of this policy
- they report any suspected misuse or problem to the Headteacher / SLT ; Online safety Officer for investigation.
- all digital communications with pupils / parents should be on a professional level and only carried out using official school systems
- Online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online safety and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Child Protection / Safeguarding Designated Person / Officer

should be trained in Online safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming

- cyber-bullying

Plus any other current issue that is highlighted via CEOP, Cheshire East DSL updates or any other service that shares the commitment to protect pupils online.

Online safety Committee

The Online safety Committee (planned for the Summer Term 2023) provides a consultative group that has wide representation from the school community, with responsibility for issues regarding Online safety and the monitoring the Online safety policy including the impact of initiatives. The group will also be responsible for regular reporting to the Board of Governors.

Members of the Online safety Committee will assist the Online safety Officer with:

- the production / review / monitoring of the school Online safety policy / documents.
- mapping and reviewing the Online safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents and the pupils about the Online safety provision

Pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy and any amendments / updates issued during the lifetime of this policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good Online safety practice when using digital technologies out of school and realise that the school's Online safety Policy covers their actions out of school, if related to their membership of the school

Parents:

Parents play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, the Parent Portal and information about national / local Online safety campaigns / literature. Parents will be encouraged to support the school in promoting good Online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website and the Parent Portal
- their children's personal devices in the school (where this is allowed)

POLICY STATEMENTS

Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in Online safety is therefore an essential part of the school's Online safety provision. Children and young people need the help and support of the school to recognise and avoid Online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce Online safety messages across the curriculum. The Online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned Online safety curriculum will be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key Online safety messages will be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Pupils will be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils will be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff will act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils will be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff will be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, will be auditable, with clear reasons for the need and certain core categories cannot be unblocked under any circumstances.

At AESG, pupils in Years 7 – 11 hand in their mobile 'phones at the start of the day and collect them at 3:45pm, unless they are attending an approved activity etc., leaving the site before the end of school. This policy aims to reduce the risk of social media abuse and engage the pupils in school activities that can stimulate their minds as well as have fun in team and individual pursuits.

The school recognises that 3G and 4G technology does not go through our web filtering system. As such we educate the pupils via PSHE lessons and assemblies about the importance of staying safe online. With the mobile 'phone policy, we aim to minimise the risks to our pupils, as much as we can, whilst in loco parentis. With iPads, we can monitor the usage of apps and respond appropriately. This usually is by the Head of Year, with DSL support.

Education – parents

Many parents and carers have only a limited understanding of Online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Communication through the Contact Newsletter
- Parents evenings / sessions with the Police
- High profile events / campaigns e.g. Safer Internet Day
- Reference/Guidance to relevant web sites / publications published on the Parent Portal
- Apple Regional Training Centre Training Sessions (E-Safety on iPad) throughout the Academic Year

Education & Training – Staff / Volunteers

It is essential that all staff receive Online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal Online safety INSETs will be made available to staff. This will be regularly updated and reinforced.
- All new staff should receive Online safety training as part of their induction programme, ensuring that they fully understand the school Online safety policy and Acceptable Use Agreements.
- The Online safety Officer will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This Online safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Online safety Officer will provide advice / guidance / training to individuals as required.

Training – Governors

Governors / Directors should take part in Online safety training / awareness sessions, with particular importance for those who are members of the Online safety Committee.

Technical – Cyber Security

Definition : What is a *Cyberattack*?

A Cyberattack is a deliberate exploitation of computer systems, technology-dependant enterprises and networks. Cyberattacks use malicious code or insecure user data to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to other cybercrimes, such as information and identity theft.

Cyberattacks may include the following consequences:

- Identity theft, fraud, extortion
- Malware, pharming, phishing, spamming, spoofing, spyware, Trojans and viruses
- Stolen hardware, such as laptops or mobile devices
- Denial-of-service and distributed denial-of-service attacks
- Breach of access
- Password sniffing
- System infiltration
- Website defacement
- Private and public Web browser exploits
- Instant messaging abuse
- Intellectual property (IP) theft or unauthorized access

Technical – Protection, Response and Insurance from Cyberattacks

The school will be responsible for ensuring that the schools externally facing infrastructure is as safe and secure as is reasonably possible.

The School's response to a Cyberattack will be dependent on the scope and type of attack faced. Responses and an IT Cyberattack action plan are part of the schools Crisis Policy.

The school will be responsible for ensuring that they have a valid Cyber Liability insurance policy and meet any and all special technical conditions applicable to this insurance policy.

The UK Government recommends annual certification via their 'Cyber Essentials' mark to prevent the vast majority of cyberattacks. Since October 2014 this certification is mandatory for suppliers of Government contracts which involve handling personal information and providing ICT products and services. Maintenance and adherence of the Cyber Essentials mark allows the school to advertise the fact that it meets the Government-endorsed standard. The school will be responsible for ensuring that this certification is awarded and maintained via an annual review.

A copy of the most recent Cyber Essentials review accompanies this policy statement and can be found as an appendix. The school will be responsible for ensuring that this certification is maintained annually.

Technical – infrastructure / equipment, filtering and monitoring

A Technical Security Policy accompanies this policy statement and can be found as an appendix

The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their Online safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted

- All users will have clearly defined access rights to school technical systems and devices.
- All users (at KS3 and above) will be provided with a username and secure password by IT Support who will keep an up to date record of users and their usernames. All users at KS2 and below will share Year group username and passwords. Users are responsible for the security of their username and password and will be required to change their password every term.
- The domain administrator passwords for the school ICT system, used by the IT Development Manager are also available to the Headteacher or other nominated SLT and kept in a secure place (the Finance Office Fireproof Safe).
- The IT Development Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the service provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes. The school has provided enhanced / differentiated user-level filtering.
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Policy Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date enterprise level virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place regarding the extent of personal use that users (staff / pupils / other users) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place that forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place regarding the minimum use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices. When possible access to removable devices is forbidden. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured

Bring Your Own Device (BYOD)

A BYOD Policy Agreement form accompanies this policy statement and can be found as an appendix

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of Online safety considerations for BYOD that need to be reviewed prior to implementing such a policy. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring. This list is not exhaustive and a BYOD policy should be in place and reference made within all relevant policies.

- The school has a set of clear expectations and responsibilities for all users
- The school adheres to the Data Protection Act principles
- All users are provided with and accept the Acceptable Use Agreement
- All network systems are secure and access for users is differentiated
- Where possible these devices will be covered by the school's normal filtering systems, while being used on the premises
- All users will use their username and password and keep this safe
- Mandatory training is undertaken for all staff
- Pupils receive training and guidance on the use of personal devices
- Regular audits and monitoring of usage will take place to ensure compliance
- Any device loss, theft, change of ownership of the device will be reported as in the BYOD policy
- Any user leaving the school will follow the process outlined within the BYOD policy

Use of digital and video images

A separate use of digital and video images policy and a Parental Consent Form both accompany this statement and can be found as appendices.

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents are welcome to take videos and digital images of their children at school events for their own personal use (as such

use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents comment on any activities involving other pupils in the digital / video images.

Staff and pupils are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.

- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Staff and Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Permission from parents will be obtained (by means of a consent form) before photographs of pupils are published on the school website.
- Pupil's work can only be published with the permission of the pupil.

Youth Produced Sexual Images (YPSI) previously known as 'Sexting'

There are several definitions of YPSI but for the purposes of this policy statement it is simply defined as:

Images or videos generated


- by children under the age of 18, or
- of children under the age of 18 that are of a sexual nature or are indecent.

Staff, pupils and parents should be made aware of the risks associated with sexting. If an incident of sexting occurs, the school will operate within the established legal framework, whilst handling the incident with the utmost care and consideration for the pupils involved. The school acknowledges that it has the power to confiscate and examine a pupil's personal digital device if there is reason to believe it contains indecent images (under the Education Act 2011). Following an incident of sexting, SLT and the school's Designated Safeguarding Lead will be informed. The Safeguarding team will investigate the incident and decide on the most appropriate course of action on a case-by case basis. Due to the serious nature of sexting incidents, the school are likely to involve outside agencies such as Social Services and the Police. See reference below.

A QUICK GUIDE | Youth Produced Sexual Images (YPSI) and inappropriate sexual contact online

Risk assessment advice to safeguard children and young people





Call the police on 101

As part of Cheshire Constabulary's commitment to working in partnership with education to keep young people safe and informed, it is important we ensure that education partners and practitioners have a clear picture of the force approach to dealing with cases of YPSI and inappropriate sexual contact online.

This information aims to support schools and partners dealing with cases of YPSI or sexual contact online to determine the need to report to police for investigation or whether matters can be dealt with outside of the law by staff, the young people involved and parents, respecting that a police response will not always be necessary.

Yes

DO ANY OF THESE FACTORS EXIST?

The presence of any aggravating factors means the matter should be reported to police to safeguard those involved and investigate the case further.

- Those involved are under 13yrs?
- An adult aged 18 or over is involved?
- Multiple victims/wider distribution
- The level of sexual nature/type of image
- Threats/coercion/harassment present
- Grooming or exploitation expected
- Wide age gaps in relationship cases

No

Where an incident has no aggravating factors, police intervention is not necessary; the matter should be resolved by staff in a balanced and proportionate way in accordance with their own safeguarding policies.

- Images produced (as part of or within) a consensual relationship for romantic or attention-seeking reasons with no identifiable aggravating factors
- Victim/suspect are not at high risk of CSE or other abuse and vulnerabilities
- No further/persistent contact from suspect
- Contact and conversation appear to be age appropriate
- Images only distributed between each other
- Type of image sent - nature/tone

Can I look at the image or content?

Only if it is completely necessary to make a full risk assessment. Conduct only with given permission from relevant staff according to school or your organisation's protocols; ensure it is carried out in the presence of someone else and that it is recorded clearly and accurately.

Can I seize a child's phone?

Yes you can. This may be necessary for the safety of the child, to reduce the risk of harm from content being shared or distributed and to make a full risk assessment.

Can I give the child's phone back to them?

Yes, if your risk assessment determines the case is low risk and falls under the exponential criteria, contact parents and agree whether they, you or the child in your/their presence **deletes all images before this is then recorded in school/organisation records**. Do not give the child the phone back until this has been done.

Will calling the police mean the child will get a criminal record?

Cheshire Constabulary will **not seek to criminalise a young person**, their safety and wellbeing is always the priority.

Only in serious cases would the police have to consider formal sanctions.

What do I do if the image is sent to me?

Delete it immediately, do not return it, show it to others or share it. Report this to your manager and the police.

What if parents aren't happy with our decision not to call the police?

Ensure parents are informed why and that they have the option to make a report themselves.

Record your investigation, assessment and rationale to enable police to support you if a report is made that we need to respond to.

Online Remote Learning

During unprecedented times, such as the school building closure due to the coronavirus outbreak, it is important that staff continue to follow the robust measures we have in place to protect staff.

Staff are expected to use their school IT facilities as much as possible. Where such action is unavoidable, staff must not save images or confidential data to their personal devices. All school platforms should be accessed in a secure manner and where a device is shared, passwords not saved.

In the event of a failure of the Staff email system an alternative backup system will be activated, so under no circumstances should personal email be used to contact a member of the school community.

In the event of such a building closure Students will be issued and are expected to conform with the 'Pupil Agreement for Online Learning from Home'. Staff will be issued and are expected to conform to the 'Staff Agreement for Online Learning from Home' (both Agreements can be found in the Appendix to this document).

It is important that Staff make their best effort to confirm the identity of the pupils they are interacting with, this helps ensure the correct students and no external 'attendees' are present.

During an extended period of Online Remote Learning the School will only make use of approved IT Solutions (such as Microsoft Teams) which provided a 'closed ecosystem' and ensure Pupil safety. Monitoring of online classes will be completed on a regular basis and a weekly report will be provided to the Online Safety Officer, real-time reporting of chat logs is provided by the SENSO tracking tool.

Data Protection

A separate Data Protection Policy Accompanies this statement.

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete

Communications

Separate Staff Code of Conduct and ICT Acceptable Use Policy Agreements accompany this statement and can be found as appendices.

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Any digital communication between staff and pupils or parents (email, chat, Teams etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class / group email addresses will be used at KS1 and KS2 while pupils at KS3 and above will be provided with individual school email addresses for educational use.
- Pupils will be taught about Online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

Separate Staff Code of Conduct and ICT Acceptable Use Policy Agreements accompany this statement and can be found as appendices.

All schools have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or LA liable to the injured party. Reasonable steps to prevent predictable harm must be in place. The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

Staff should ensure that:

- No reference should be made in social media to pupils, parents or school staff
- They do not engage in online discussion on personal matters relating to members of the school community

- They use IT Support and other technical expertise in the school
- Personal opinions should not be attributed to the school or LA
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

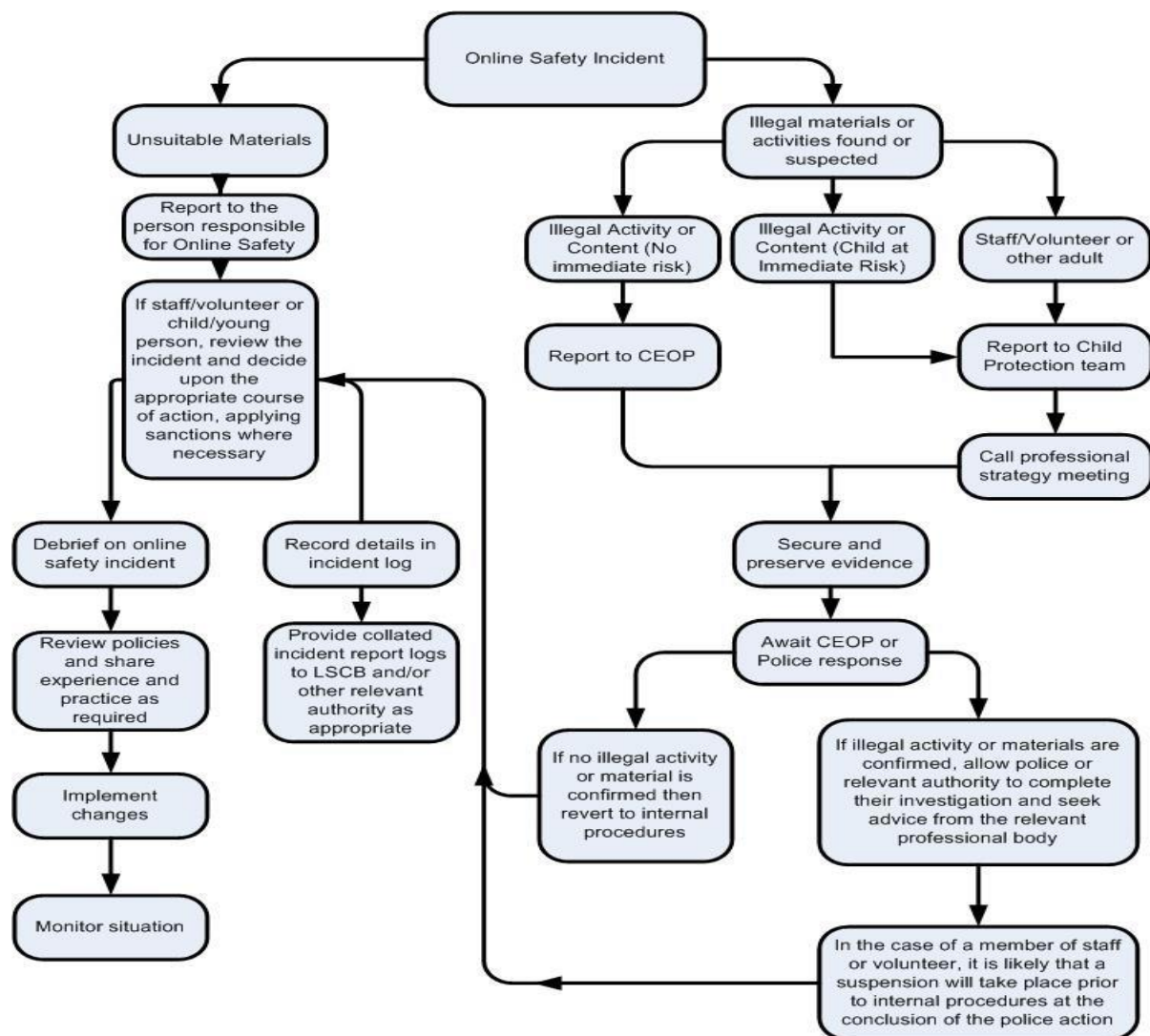
The school's use of social media for professional purposes will be checked regularly by the SLT and Online safety committee to ensure compliance with the Acceptable Use Policy Agreement.

RESPONDING TO INCIDENTS OF MISUSE

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).

- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
 - Internal response or discipline procedures
 - Involvement by LA or national / local organisation (as relevant).
 - Police involvement and/or action
- **If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
 - incidents of ‘grooming’ behaviour
 - the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
 - criminally racist material
- other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures.

Pupil Acceptable Use Policy Agreement Template – for younger pupils (EYFS / KS1)

This is how we stay safe when we use computers:

I will ask a teacher or suitable adult if I want to use the computers

I will only use activities that a teacher or suitable adult has told or allowed me to use.

I will take care of the computer and other equipment

I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.

I will tell a teacher or suitable adult if I see something that upsets me on the screen.

I know that if I break the rules I might not be allowed to use a computer.

Signed (child):.....

Signed (parent):

Acceptable Use Policy for Technology – Pupils in Prep, Pre Prep and EYFS

Revision: April 2023



ALDERLEY EDGE
SCHOOL FOR GIRLS

Dear Parents,

At AESG, we believe there are clear benefits to using technology in the classroom to enhance the girls' learning experience. It is also vital that the girls understand how they can keep themselves, and our School systems, safe from harm while doing so. We have some simple and sensible rules that outline how we expect all our Prep, Pre Prep and EYFS pupils to behave while using technology, and these are set out below.

Of course, technology safety is covered in an age-appropriate way at every stage of the School and we ask for parents' help to reinforce these important messages. Please complete the acknowledgement on our Parent Portal to confirm that you have read these rules and have discussed them with your daughter(s). You can find lots of online safety tips, advice and resources at the UK Safer Internet Centre: <https://www.saferinternet.org.uk/>. If you have any queries, please contact the School.

Yours faithfully,

Mr T Marchington
Deputy Head (Prep)

The School will:

- provide internet access at School via computer suites and iPads connected to Wi-Fi;
- provide internet filtering / blocking of inappropriate materials when using the School's Internet connection, using a Government-approved system;
- implement further deployment and monitoring systems to make resources available to girls and provide a safe environment for the use of technology;
- provide a suitable Microsoft 365 licence and account to enable the use of Microsoft Office apps;
- provide secure access to the School's network storage, using the Foldr app on iPads;
- provide any paid-for apps required by teachers for the courses studied at School.

We ask girls and their parents to understand that:

- the standard of behaviour expected while using technology should be equal to that expected anywhere else within School; it reflects on pupils and on the School;
- Internet access from within School is filtered and monitored, and any websites and apps that a girl accesses in School can be viewed by their class teacher or by another member of staff;
- failure to follow these rules may result in disciplinary action, as detailed in the School's policies;
- the IT Support team at Alderley Edge School for Girls will do their best to assist with technical queries, but cannot assume an obligation for such support, and cannot accept liability for any

modifications made to personal equipment as a result of establishing a connection to our systems.

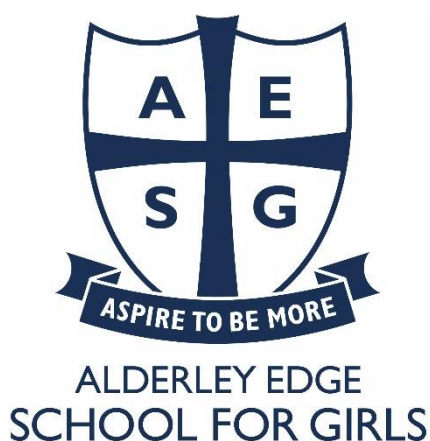
Girls' responsibilities:

- Girls must only use a computer or iPad in School when they have been given permission by their class teacher or another member of staff;
 - Girls must take care of electronic equipment, and must notify their class teacher or a member of the IT Support staff immediately if anything is damaged or goes missing;
 - Girls must only use School technology in ways that are responsible, appropriate and educational. If they see anything on a computer or iPad that makes them uncomfortable, worried or upset, or if they access inappropriate content by mistake, they should let their teacher know immediately;
 - Girls must treat everyone with respect at all times; when online or using a device, they should treat others as if they were talking to them face-to-face, and any messages (or other information they upload) must be kind, responsible and respectful;
 - Girls must choose a sensible place to work from and dress appropriately if working from home;
 - Girls must ensure that they check their sources of information, understanding that some websites and other online information can be misleading, biased, out-of-date or just wrong;
 - Girls must log off a School device (computer or iPad) when they have finished using it;
 - Girls must ask their class teacher or another member of staff if they are unsure before doing anything using technology.
-
- Girls must not use School systems for non-School / non-lesson communications;
 - Girls must not allow food or drinks near any School technology, as they may cause damage to it;
 - Girls must not link equipment to any other technology within School without permission;
 - Girls must not provide their School log-in passwords to anyone else under any circumstances, and must not attempt to access systems using anyone else's log-in details. Ideally, passwords should be remembered and not written down or saved anywhere, so that they cannot be accessed by others;
 - Girls must not attempt to bypass the School's Internet filtering, or any other system in place for their safety or that of others around them;
 - Girls must not open any file or click on any hyperlinks without being sure it is safe to do so, understanding that some files and website may contain code that can damage devices or erase data (malware or viruses), and will always double-check before clicking;
 - Girls must not share any personal information anywhere online unless a trusted adult has given them permission to do so;
 - Girls must never say anything online that could hurt, embarrass or isolate another person, understanding that bullying will be dealt with immediately and in line with School policies.

MOBILE PHONES – Mobile phones may not be used by girls during School time under any circumstances and for any purpose (calls, messages etc). Girls are not encouraged to bring mobile phones into School, and may do so only if required as a safety measure when travelling to and from School. Any phones brought in for this purpose should be

switched off and handed to the class teacher immediately upon arrival and collected upon leaving. The School cannot be held responsible for any devices brought onto the premises.

Please discuss these rules with your daughter(s), and then complete the acknowledgement on the Parent Portal. This is located on the Electronic Forms page in the School Information section. If you have any difficulties accessing the Portal, please contact our IT Support team: itsupport@aesg.co.uk. Thank you.



Acceptable Use Policy for Technology – Pupils in Senior School

Revised September 2022 CW / NP

We believe there are clear benefits to using technology in the classroom to enhance your learning experience. Senior School girls connect their own iPads to the School network and services and have access to School computers. We have some simple and sensible rules that we expect all girls to follow while using technology within School, and we ask you to sign to confirm that you have read and understand them. This form sets out the School's responsibilities to you and your responsibilities to the School in return. If you need this form in any other format, please let IT Support know.

School's responsibilities to you:

- **We** will provide internet access at School via computer suites and Wi-Fi;
- **We** will provide internet filtering / blocking of inappropriate materials when using the School's Internet connection, using a Government-approved system;
- **We** will implement further deployment and monitoring systems to make resources available to girls and provide a safe environment for the use of technology;
- **We** will provide Senior School girls with an academic email account (<username>@aesg.info);
- **We** will provide a suitable Microsoft 365 licence and account to enable the installation of Microsoft Office and Teams on girls' iPads;
- **We** will provide secure access to the School's network storage via the Foldr app;
- **We** will provide any paid-for apps required by your teachers for the courses studied at School;
- **We** will provide the training required by girls to make the best use of their iPads;
- **We** will meet all requirements for Keeping Children Safe in Education (September 2022) plus any future updates.

Your responsibilities to School:

- **You agree** only to use your own iPad, and not to lend your iPad to other girls;
- **You agree** to take care of your iPad and ensure it is kept safe and well protected – we strongly recommend that it is in a sturdy case. AESG can accept no responsibility for any damage or loss. You must notify a teacher or a member of the IT Support team immediately if your iPad is damaged or goes missing;
- **You agree** to bring your iPad into School fully charged every day; the School cannot guarantee to be able to lend you an iPad if you forget yours, or if it should run out of charge. You can charge your iPad in School at IT Support if necessary; personal chargers should not be used in School;
- **You agree** to allow your iPad to be connected to your teacher's using Apple Classroom on request;
- **You agree** only to use your iPad and any other School technology in ways that are responsible, appropriate and educational. Any content (including photos and videos) stored on your iPad, or on its

case or other decorations (such as stickers), must be wholly appropriate for our School environment. You may be required to remove apps with known e-safety or security issues. If you access inappropriate content by mistake, you should let your teacher know immediately;

Your responsibilities to School (continued):

- **You agree** not to attempt to bypass our Internet filtering or any other system in place for your safety or that of others around you. **The use of virtual private networks (VPN) apps is strictly prohibited** and checks will be made regularly. Internet access from within School is filtered and/or monitored, and any websites and apps that you access in School will be logged;
- **You agree** not to use Microsoft Teams for non-School / non-lesson communications. Channels for smaller group conversations must only be set up with the express permission of your teacher. Please note that all Teams chat activity is monitored;
- **You agree** to keep food and drinks away from your iPad and any other School technology, as they may cause damage to electrical equipment;
- **You agree** to ensure your iPad has a Passcode and/or Touch ID in order to keep it locked when not in use;
- **You agree** to ensure your School email account is connected to your iPad, to enable reliable, safe communication with teachers and other School staff;
- **You agree** to install the School's Mobile Device Management (MDM) application – currently Meraki Systems Manager. This app enables us to secure your work if your iPad is ever lost or stolen, track your iPad if it is mislaid within School, and monitors for prohibited apps. (It does NOT allow us to see your photos, personal messages etc.) Once configured, it must be left on your iPad;
- **You agree** not to link your iPad to any other technology (for example Apple Watches or other tablets) within School;

- **You understand** that the standard of your behaviour while using technology is expected to be equal to that expected anywhere else within School;
- **You understand** that the use of your iPad in School lessons is at the discretion of your class teacher. When not in use, it should be locked, on silent, with the case closed and face down;
- **You understand** that girls in Years 7-9 should not access their iPads in Form Time, break time or at lunchtime unless under the supervision of a member of staff;
- **You understand** the rules set out by the School and will follow them to the best of your ability;
- **You understand** that failure to follow these sensible rules may result in your being subject to disciplinary action, as detailed in the School's policies;
- **You understand** that in exceptional circumstances (for example, to investigate a potential e-safety or disciplinary issue), you may be required by a member of the School's Senior Leadership Team to allow teaching or IT Support staff access to your iPad and provide your iPad passcode to them;
- **You understand** that the IT Support team at Alderley Edge School for Girls will do their best to assist girls and families with their technical issues, but cannot assume an obligation for such support, and cannot

accept liability for any modifications made to equipment as a result of establishing a connection to our systems.

Please sign below to say that you have read, understand and agree to follow our rules:

_____ **Print Name** _____ **Date** _____ **Signature**
(block capitals)

ICT Acceptable Use for Staff, Visitors and Volunteers

Whole School and EYFS

Reviewed: November 2022 (CW / NP)

Governor Review: November 2022

Staff (and Volunteer) Acceptable Use Policy Agreement (AUP)

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

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;
- that **school ICT systems and users are protected from accidental or deliberate misuse** that could put the security of the systems and users at risk;
- that **staff are protected from potential risk in their use of ICT in their everyday work**;
- that the School will meet all requirements for **Keeping Children Safe in Education** (September 2022) plus any future updates.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for pupils' learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use the School's ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the School will monitor my use of the ICT systems, email and other digital communications.

- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. iPads, laptops, email etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it. I will utilise multi-factor authentication apps as required by the School.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person (DSL, Headmistress or Chair of Governors).
- I will ensure that I log off all online services and the school network computers after I have finished using them.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website or social media) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils and parents using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will avoid using other people's devices, particularly those used by students, unless absolutely essential.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use any mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will ensure I save my files in the appropriate folder on the appropriate network drive and will not save files to a computer's desktop.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will avoid making large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.

- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the data protection policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based, Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school-sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action and in the event of illegal activities, the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Visitor / Volunteer Name

Signed

Date

BRING YOUR OWN DEVICE POLICY AGREEMENT – All Users

Alderley Edge School for Girls allows staff and students to attach personal devices to the WIRELESS network at the discretion of the schools' management. This agreement form should be used by staff and students who wish to request a personal device be attached to the school's WIRELESS network. All policy and regulations are to be adhered to strictly.

I understand that Alderley Edge School for Girls assumes no obligation for the support, either onsite or by telephone, of personal electronic equipment neither will it accept any liability for modifications made to the equipment as a result of establishing a connection.

- I assume all liability when installing or uninstalling any software and do so at my own risk. I am responsible for adhering to copyright and licensing laws and guidelines for all software on my personal equipment.
- I must have current antivirus software installed on my computer and must continue to have up to date virus definitions installed and configured (subject to technical services approval).
- I cannot have any network services (telnet, DNS, DHCP, web services, file-sharing programs [KaZaa, LimeWire, etc.]); or network utilities running on my system.
- I understand that no personal network routers, access points, switches, hubs, network printers, or any other device, may be used on the AESG network at any time.
- I understand that at no time can AESG equipment be attached to my personal equipment except for that specifically authorised by the IT Technical Support Team.
- I understand that my actions while using my personal equipment on the AESG network are governed by the schools' policy and regulations.
- I will not store any confidential school data on my personal equipment.
- I will not hold the school liable for theft, damage or loss of personal equipment.
- I understand this approval is granted for the current school year and must be reapplied for annually.

I have read and accept the school's policies and procedures listed above regarding connectivity to the AESG WIRELESS network and I agree to abide by them. I understand that should I fail to comply with regulations, my access privileges may be revoked and/or appropriate legal action may be taken.

Staff / Volunteer /Pupil Name

Signed

Date

USE OF PHOTOGRAPHIC, DIGITAL AND VIDEO IMAGES POLICY

Whole School & EYFS

Scope

This policy is addressed to all members of staff, visitors, parents, and pupils. The policy relates to the taking, using and storing of images of children:

- on School premises; or
- in connection with School activities; or
- for other legitimate purposes of the School.

It covers the activities of staff, pupils, parents, and visitors to the School.

Images: this expression in relation to pupils includes:

- photographs and digital photographs;
- video or film clips;
- images captured by mobile phones with a "camera" facility;
- webcams

*Taking images: **this** expression includes, unless otherwise stated, making, editing, using, exhibiting and storing images of pupils.*

Aims

The aims of this policy are:

- to promote safety and welfare and respect for others;
- to ensure a sensible balance between privacy, creative self-expression and routine collating of information;
- to comply with the law and good practice without adhering to unnecessary bureaucratic procedures.

Privacy No person is authorised to take images of children that: □ might cause embarrassment or distress; or

- are associated with distressing or sensitive issues; or
- are unnecessarily intrusive.

Journalism:

Filming and photography by television or newspaper journalists will take place only with the consent of the Headmistress and under appropriate supervision. When images are taken for publication by television or newspaper journalists, children will only be named if there is a particular reason to do so (for example if they have won a prize) and home addresses will not be given out.

Promotional material

It is an implied term of the contract for educational services which exists between the School and the parents of a pupil, that photographs of the pupil may be taken and used by the School in accordance

with normal custom and practice. Such custom and practice will include: set piece photographs of the School, house, team, theatre cast and snapshots of School activities. It has also been custom and practice for independent schools to use images of their pupils for marketing purposes, such as in prospectuses and promotional videos or displays on its website.

The School's terms and conditions specify that parents who do not want their child's photograph or image to appear in any of the School's materials must have indicated this on the signed Consent form.

Where a Pupil's photograph is used in the School's promotional material, the School will not use the Pupil's full name in connection with that photograph.

Taking of images by parents and friends at school productions

Parents and friends often wish to take images of their children at school productions, concerts or sporting activities. Courtesy and good manners require that the following rules are respected:

- they must first seek permission of a pupil/group of pupils before taking the digital image or video
- If visitors ask whether they can take photographs, they should be reminded that whilst it is permissible under the Data Protection Act 1998 to take photographs for personal use, publication of such images may be unlawful (see Appendix 1 below);
- where a play or concert or other event is subject to copyright and performing rights restrictions, visitors will not be permitted to take images, photographs or video film. Official photographs or videos may be available for sale, however.

Seeking consent

Although consent of parent(s) or pupils is not always a legal requirement, the School will seek express prior written consent:

- for use of portrait style images of pupils;
- for use of pupils' images by or with commercial sponsors;
- where a pupil wishes to use images of other pupils as part of GCSE or A-level coursework;
- where the School might receive a payment or other tangible benefit for allowing the use of a photograph, for example, providing a photograph to the media where the pupil has subsequently become a celebrity.

Where consent is required as above we will obtain such consent from at least one parent [and/or] the pupil, provided the pupil is of sufficient maturity and understanding to provide consent. Pupils aged 16 and above will normally be considered to be capable of giving or withholding consent.

Photographs as part of pupil records

All pupils in Year 7 have a passport-style photograph taken by AESG which forms part of the pupil's personal record. These images are subject to the Data Protection Act 1998 (see Appendix 1) and will therefore:

- be stored securely;
- not be used for any other purpose without the consent of the pupil or his or her parent(s);
- not be shown, copied or given to any unauthorised person.

Pupil use of cameras, mobile phones and other personal devices with a camera facility Pupils in the Prep School are forbidden to operate a mobile phone or any other personal device with a camera facility during school time.

Pupils in Year 7 to Year 11 are forbidden to operate mobile phones in lesson time. These pupils are allowed to operate mobile phones during break, in designated areas of the school, however, pupils are forbidden to use the camera facility to take photos of other pupils and/or staff members.

Year 12 and 13 pupils may only take images with mobile phones, cameras or other personal devices with the express permission of all those appearing in the image. All pupils must allow staff access to images stored on mobile phones and/or cameras and must delete images if requested to do so.

Using photographic material of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline.

Staff use of cameras, mobile phones and other personal devices with a camera facility.

Staff, visitors and parents must not take images of pupils who have not given permission on the signed Consent Form .

It is the responsibility of staff to ensure they are aware of all pupils that have not given consent to allow digital and video images of them being taken.

In the instance of staff taking images of pupils and pupils' work in lessons or when out on trips, they must use a school owned device and NOT their own personal device.

No images of pupils should be stored on staff personal devices.

Child Protection

When publishing images of children in school documents or on the website, care will be taken to minimise the risk of such images being modified to create inappropriate or indecent images. The Designated Officer for Child Protection, Mrs Caroline Wood, can give specific advice as requested.

Staff will be mindful of child protection issues and will raise concerns with the Designated Officer for Child Protection if they become aware of anyone:

- taking an unusually large number of images;
- taking images in inappropriate settings such as cloakrooms, toilets or changing areas;
- taking images of children who are apparently unaware that they are being photographed or filmed.

Legal framework May 2008

Privacy

The law does not restrict the general right of individuals to take photographic or video images of other people. The restrictions that exist relate to wrongful exploitation.

David Murray (By his litigation friends (1) Neil Murray (2) Joanne Murray v Big Pictures (UK) Limited [2008] EWCA Civ 446

Dr and Mrs Murray (who is better known as J. K. Rowling) brought a case against a photographic agency on behalf of their 19 month old son David. They objected to the publication of photographs taken with a long-range camera whilst the family were out walking and then sitting in a café. The claim was struck out by a High Court judge on the grounds that there was no arguable case for privacy in these

circumstances, based on previous case law. The Court of Appeal, however, ruled that the claim can go ahead.

The Court confirmed that a person does not generally have a right to prevent photographs being taken and does not have a right to any images of themselves. However, the Court felt that even where photographs were taken in a public place and were not in themselves embarrassing or humiliating, it was at least arguable that a child could reasonably expect that the press would not target him and publish photographs of him simply because of his famous parent.

Campbell v MGN Ltd [2004] UKHL 22

The House of Lords confirmed that publishing a photograph of Ms Naomi Campbell leaving a drug addiction clinic contravened her right to privacy.

Douglas, Zeta-Jones and Northern & Shell Plc v Hello! and others [2005] EWCA Civ 595 The Court of Appeal followed the Campbell case by ruling that the publication of unauthorised photographs of Michael Douglas and Catherine Zeta-Jones' wedding reception breached the couple's right to privacy. The wedding was a private occasion even though the couple had agreed to allow the publication of authorised photographs.

Data protection

The Information Commissioner has clarified that the Data Protection Act 1998 is unlikely to apply to many cases where photographs are taken in schools.

- Photographs taken for official school use may be caught by the Act. These are likely to include photographs taken for security passes. Pupils should be informed of the purpose for which the photographs are taken and the photographs themselves should be stored securely and not used for other purposes. However, a photograph of a group of pupils taking part in a lesson to be used in the school prospectus does not constitute personal data and the Act will not apply.
- Photographs taken purely for personal use are exempt from the Act. This would include photographs taken by parents or friends intended to be put in the family photo album.
- Photographs of school events taken by the local newspaper are unlikely to be caught by the Act. There are also exemptions for journalistic use. However, it is good practice to notify parents that the press will be attending certain events.

□

The court in the J. K. Rowling case described above also considered the Data Protection Act in this context. If the court that eventually hears the full claim rules that the child's right to privacy has been breached then the "processing" of the material will be unfair and contrary to the Data Protection principles.

Further information is available on www.informationcommissioner.gov.uk.

Child protection

It is a criminal offence under the Protection of Children Act 1978, as amended, to take indecent photographs of a child. A "child" is anyone under 18 although there are defences involving children over 16 in a marital (or similar) relationship. The definition of "photograph" includes images on a mobile phone or stored on a computer and also includes "pseudo photographs" where images have been manipulated. It is also an offence for someone to distribute or show such images or to have them in his possession with the intention of showing them to himself or others.

The government has recently announced proposals to amend the law so that all images of child sexual abuse, including drawings and computer-generated images of child abuse will be illegal. Offenders holding such images will face criminal charges and up to three years in prison. The distribution or sale of such material is currently illegal under the Obscene Publications Act 1959, and possession of photos of child pornography is unlawful. However, it is not yet a criminal offence to possess drawings and

computer-generated images of child abuse. The proposals will create a new criminal offence to possess drawings and computer-generated images of under-aged children in sexual activity.

Consent: Publication of Photographs & other forms of Media and Consent for Communications

During the course of daily school life, there are many occasions when members of staff may need to take a photographic record of classroom activities for display purposes and to record pupils work. This is often the case for those children who are involved in extra-curricular activities or who go on school trips.

The School also uses photographs, video footage and audio clips for marketing purposes both internally and externally in order to celebrate the achievements of pupils and to promote the success of our school.

We would like to ensure that the School has your full permission to use the photographs, video or sound recordings. The School is aware of its Safeguarding obligations and ensures that images are stored safely on the school network which is accessible to staff only.

The School will commission images (electronic and/or in the form of prints) and filming in several ways via:

- A member of staff using a school camera, iPad, mobile phone or recording equipment.
- A parent who has the permission of the School to take images using school equipment.
- A commissioned freelance photographer or school photography company.
- By a third party such as a speaker, business, charity or associated organisation during a school associated event or trip.

Photographs and footage may be used in conjunction with internal or external materials such as:

- Advertising campaigns which may appear in magazines, billboards or on public transport in the local area.
- Advertorial or editorial features that are issued to the media such as local newspapers, magazines on online news sites. These features often include pupil full names, year group or form and home town.
- Aspire Magazine, our printed and online termly newsletter. Aspire Magazine often includes pupil full names, year group or form. Please be aware that this publication can be viewed and downloaded from the school website.
- Display materials in school such as the Celebration Board, posters, noticeboards and on the digital signage screens.
- Marketing materials including prospectuses, booklets to parents, postcards and additional literature.
- Radio, television interviews or sound bites e.g. Results Day interviews or concert recordings
- School videos – either internally or professionally produced.

continued overleaf

- Our official Social Media accounts - Facebook, Twitter and Instagram. Pupil first names, surname initial if required and year group or form may also be referenced.
- The school website www.aesg.co.uk
- Video accounts such as You Tube and Vimeo.
- Weekly e-newsletters to parents via Mailchimp, namely Contact (Senior School & Sixth Form) or Bulletin (Early Years & Sixth Form). Pupil first names, surname initial if required and year group or form may also be referenced.

Personal details will not be published other than those stated above and, when possible, the School will aim to make contact with you out of courtesy should your child be used in an external advertising campaign.

We hope you will support us with our use of photographs and media. It can often cause upset if we need to ask a pupil to leave a photo opportunity or activity due to not having the appropriate parental consent.



Certificate of Consent: Publication of Photographs & other forms of Media and Consent for Communications

Parent name:

Child(s) name:

Signature:

Date:

Yes – I give consent for the school to take and use images or footage of my child(s) as outlined in the letter.

No – I do not give consent for the school to take or use images or footage of my child(s). Please be aware that this means your child will be asked to leave group photos and will miss out on opportunities to celebrate their successes internally and externally.

No – I do not give consent for the school to take or use images or footage of my child(s). I do however provide consent for my child to have an individual school photo (annual) and be a part of the whole school photo which will be available in school and for parents to purchase.

I understand that by signing this consent form, the School will be able to use images of my child(s) and will apply for the duration of my child's time at AESG and after she has left unless I notify the school otherwise.

DATA PROTECTION POLICY

Whole School & EYFS

Rationale:

The growth in the use of personal data has many benefits both for society, and for the individual. However, whenever personal data is collected and used, people's lives can be adversely affected if errors occur in that data. Also, if data is not kept secure, privacy can be affected. Therefore, it is vital that those who collect and use personal data comply with the Data Protection Act.

The Data Protection Act 1998 applies to 'personal data' about identifiable living individuals, and covers 'obtaining', 'holding' and 'disclosing' this data.

1. General Statement of Duties

Alderley Edge School for Girls is required to process relevant personal data regarding staff as part of its operation and shall take all reasonable steps to do so in accordance with this Policy.

2. Data Protection Controller

The School has appointed a Data Protection Controller ("DPC") – the Director of Finance and Operations - who will endeavour to ensure that all personal data is processed in compliance with this Policy and the Principles of the Data Protection Act 1998.

3. The Principles

The School shall, so far as is reasonably practicable, comply with the Data Protection Principles ("the Principles") contained in the Data Protection Act to ensure all personal data is:

- Processed fairly and lawfully.
- Obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
- Adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Accurate and, where necessary, kept up to date.
- Not kept for longer than is necessary for that purpose or those purposes.
- Processed in accordance with the rights of data subjects under this Act Kept secure.
- Not transferred to other countries without adequate protection

4. Personal Data

Personal data covers both facts and opinions about the individual. It also includes information necessary for employment purposes such as name, address, contact details and details required for payment of salary

5. Processing of Personal Data

Consent may be required from a member of staff for the processing of personal data, unless processing is necessary for the performance of the contract of employment. Any information which falls under the definition of personal data and is not otherwise exempt will remain confidential and will only be disclosed to third parties with the consent of the member of staff.

6. Sensitive personal Data

The School may, from time to time, be required to process sensitive personal data regarding a member of staff. Sensitive personal data includes medical information and data relating to religion, race, trade union membership and criminal records and proceedings. Where sensitive personal data is processed by the School, the explicit consent of the member of staff will generally be required in writing.

7. Rights of Access to Information

Any member of staff wishing to access their personal data should put their request in writing to the DPC. The School will endeavour to respond to any such written requests as soon as is reasonably practicable and in any event, within 40 days for access to records and 21 days to provide a reply to an access to information request.

8. Exemptions

Certain data is exempted from the provisions of the Data Protection Act which includes the following:

- The prevention or detection of crime;
- The assessment of any tax or duty;
- Where the processing is necessary to exercise a right or obligation conferred or imposed by law upon the School.

The above are examples only of some of the exemptions under the Act. Any further information on exemptions should be sought from the DPC.

9. Accuracy

The School will endeavour to ensure that all personal data held in relation to members of staff is accurate. Staff must notify the DPC of any changes to information held about them. A member of staff has the right to request that inaccurate information about them is erased.

10. Enforcement

If a member of staff believes that the School has not complied with this Policy or acted otherwise than in accordance with the Data Protection Act, the member of staff should utilise the School grievance procedure and should also notify the DPC.

Objectives:

The School aims to comply with the requirements of the Data Protection Act 1998 by:

- Ensuring that members of staff are made aware of the Act.
- Ensuring that adequate training and / or documentation is made available to all staff who may process 'personal data', in order that they are able to fully understand the requirements of the Act.

Further information can be obtained from www.ico.gov.uk

TECHNICAL SECURITY POLICY

Whole School & EYFS

Password Security

Introduction

The school will be responsible for ensuring that the network is as safe and secure as is reasonably possible and that:

- Users can only access data to which they have right of access
- No user should be able to access another's files, without permission (or as allowed for monitoring purposes within the school's policies).
- Access to personal data is securely controlled in line with the school's personal data policy
- Logs are maintained of access by users and of their actions while users of the system

A safe and secure username / password system is essential if the above is to be established and will apply to all school ICT systems, including email and online learning platforms.

Responsibilities

The management of the password security policy will be the responsibility of the IT Development Manager.

All users (staff and students) will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security. The only exception to this is the 'group-logons' used by the Prep School Key Stages which have extremely limited network access.

Passwords for new users, and replacement passwords for existing users are allocated by the IT Support Department. Any changes carried out must be notified to the manager of the password security policy (above).

Users will change their passwords every 90 days.

Training / Awareness

It is essential that users should be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access / data loss. This should apply to even the youngest of users, even when class log-ons are being used.

Members of staff will be made aware of the school's password policy:

- At induction
- Through the school's Online safety policy and password security policy
- Through the Acceptable Use Agreement

Pupils will be made aware of the school's password policy:

- In Computing and / or Online safety lessons (the school should describe how this will take place)
- Through the Acceptable Use Agreement

Policy Statements

All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the IT Development Manager and will be reviewed by the Online safety Committee (or other group).

All users (at KS2 and above) will be provided with a username and password by the IT Support Department who will keep an up to date record of users and their usernames. Users will be required to change their password every 90 days. Students using Prep School 'group-logons' should always be supervised and members of staff should never use these logons for their own network access.

The following rules apply to the use of passwords: (schools will need to take account of LA guidance and the level of security required factored against the ease of access required for users):

- Passwords must be changed every 90 days
- The last four passwords cannot be re-used
- The password should be a minimum of 8 characters long and
- Must include three of – uppercase character, lowercase character, number, special character
- The account should be "locked out" following six successive incorrect log-on attempts
- Temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on
- Passwords shall not be displayed on screen, and shall be securely hashed (use of oneway encryption)
- Requests for password changes should be authenticated by the IT Development Manager to ensure that the new password can only be passed to the genuine user.
- The "administrator" passwords for the school ICT system, used by the IT Development Manager must also be available to the Bursar and kept in a secure place (the school safe). The school should never allow one user to have sole administrator access.

Audit / Monitoring / Reporting / Review

The IT Development Manager will ensure that full records are kept of:

- User Ids and requests for password changes
- User log-ons
- Security incidents related to this policy
- All server log, workstation and other device logs for a minimum of three months.

In the event of a serious security incident, the police may request and will be allowed access to passwords used for encryption.

User lists, IDs and other security related information must be given the highest security classification and stored in a secure manner.
These records will be reviewed by the Online safety Committee.

Internet Filtering Security

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Responsibilities

The responsibility for the management of the school's filtering policy will be held by the IT Development Manager. They will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must:

- be logged in change control logs
- be reported to a second responsible person (IT Support Technician or Data Development Manager):

All users have a responsibility to report immediately to the IT Development Manager any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Education / Training / Awareness

Students will be made aware of the importance of filtering systems through the Online safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- Signing the AUP
- Induction training
- Staff meetings, briefings, Inset.

Parents will be informed of the school's filtering policy through the Acceptable Use agreement and through Online safety awareness sessions / newsletter etc.

Changes to the Filtering System

- All changes to the web filter system must be logged as a job request via the IT Helpdesk system (for audit purposes).
- Only members of staff are allowed to request changes to the web filter system.
- All requests will be reviewed by the IT Development Manager to evaluate risk and ensure there is a strong educational reason for the change. Where this is not clear the decision will be referred to SLT.

- A complete list of any whitelisted website (or other changes to the web filtering system) can be viewed by SLT or the Online safety Governor at any time.

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the IT Development Manager who will decide whether to make school level changes (as above).

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School Online safety Policy and the Acceptable Use agreement. Monitoring will take place as follows: The school utilises Sophos web tracking software which can track individual users web activity on any workstation or BYOD device throughout the school.

Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- The Senior Management Team
- Online safety Committee
- Online safety Governor / Governors committee

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

Cyber Essentials IT Review

The Initial Cyber Essentials Assessment (last renewed July 2022) and relevant school responses can be found below

Boundary Firewalls and Internet Gateways

- 1) Have one or more firewalls (or similar network devices) been installed on the boundary of the organisation's internal network(s)? **Yes**
- 2) Has the default administrative password of the firewall (or equivalent network device) been changed to an alternative strong password? **Yes**
- 3) Has each open connection (i.e. allowed ports and services) on the firewall been subject to approval by an authorised business representative and documented (including an explanation of business need)? **Yes, always**
- 4) Have vulnerable services (e.g. Server Message Block (SMB), NetBIOS, Telnet, TFTP, RPC, rlogin, rsh or rexec) been disabled (blocked) by default and do those that are allowed have a business justification? **Yes, always**
- 5) Have firewall rules that are no longer required been removed or disabled? **Yes**
- 6) Are firewall rules subject to regular review? **Yes**
- 7) Have computers that do not need to connect to the Internet been prevented from initiating connections to the Internet (default deny)? **Yes**
- 8) Has the administrative interface used to manage the boundary firewall been configured such that it is not accessible from the Internet? **Yes**

Secure Configuration

- 1) Are unnecessary user accounts on internal workstations (or equivalent Active Directory domain) (e.g. guest, previous employees) removed or disabled? **Yes, always**
- 2) Have default passwords for any user accounts been changed to suitably strong passwords? **Yes, always**
- 3) Are strong, complex passwords defined in policy and enforced technically for all users and administrators? **Yes, always**
- 4) Has the auto-run feature been disabled (to prevent software programs running automatically when removable storage media is connected to a computer or network folders are mounted)? **Yes, always**
- 5) Has unnecessary (frequently vendor-bundled) software been removed or disabled, and do systems only have software on them that is required to meet business requirements? **Yes, always**
- 6) Is all additional software added to workstations approved by IT or management staff prior to installation, and are standard users prevented from installing software? **Yes, always**
- 7) Has a personal firewall (or equivalent) been enabled on desktop PCs and laptops, and configured to disable (block) unapproved connections by default? **Yes, always**
- 8) Are all user workstations built from a fully hardened base platform to ensure consistency and security across the estate? **Yes, always**
- 9) Are Active Directory (or equivalent directory services tools) controls used to centralise the management and deployment of hardening and lockdown policies? **Yes, always**
- 10) Are proxy servers used to provide controlled access to the Internet for relevant machines and users? **Yes, always**
- 11) Is an offline backup or file journaling policy and solution in place to provide protection against malware that encrypts user data files? **Yes, always**
- 12) Is there a corporate policy on log retention and the centralised storage and management of log information? **Yes**
- 13) Are log files retained for operating systems on both servers and workstations? **Yes, always**

- 14) Are log files retained for relevant applications on both servers (including DHCP logs) and workstations for a period of at least three months? **Yes, always**
- 15) Are Internet access (for both web and mail) log files retained for a period of least three months? **Yes, always**
- 16) Are mobile devices and tablets managed centrally to provide remote wiping and locking in the event of loss or theft? **Yes**
- 17) Is a mobile device management solution in place for hardening and controlling all mobile platforms in use within the organisation? **Yes**

Access Control

- 1) Is user account creation subject to a full provisioning and approval process? **Yes**
- 2) Are system administrative access privileges restricted to a limited number of authorised individuals? **Yes**
- 3) Are user accounts assigned to specific individuals and are staff trained not to disclose their password to anyone? **Yes**
- 4) Are all administrative accounts (including service accounts) only used to perform legitimate administrative activities, with no access granted to external email or the Internet? **Yes**
- 5) Are system administrative accounts (including service accounts) configured to require a password change at least every 60 days and to use suitably complex passwords? **In most cases regarding the password change, in all cases do administrative accounts have suitably complex passwords.**
- 6) Where password changes are required for system administrative accounts (including service accounts), how often are changes required? **Every 180 days**
- 7) Are users authenticated using suitably strong passwords, as a minimum, before being granted access to applications and computers? **Yes**
- 8) Are user accounts removed or disabled when no longer required (e.g. when an individual changes role or leaves the organisation) or after a predefined period of inactivity (e.g. 3 months)? **Yes**
- 9) Are data shares (shared drives) configured to provide access strictly linked to job function in order to maintain the security of information held within sensitive business functions such as HR and Finance? **Yes**

Malware Protection

- 1) Has anti-virus or malware protection software been installed on all computers that are connected to or capable of connecting to the Internet? **Yes**
- 2) Has anti-virus or malware protection software (including program/enginecode and malware signature files) been kept up-to-date (either by configuring it to update automatically or through the use of centrally managed service)? **Yes**
- 3) Has anti-virus or malware protection software been configured to scan files automatically upon access (including when downloading and opening files, accessing files on removable storage media or a network folder) and scan web pages when accessed (via a web browser)? **Yes**
- 4) Has malware protection software been configured to perform regular periodic scans (e.g. daily)? **Yes**
- 5) Are users prevented from executing programs from areas of the disk to which they have write access? **In most cases**
- 6) Are users prevented from executing programs from areas of the disk to which temporary Internet files are downloaded? **Yes**

Patch Management

- 1) Do you apply security patches to software running on computers and network devices? **Yes**
- 2) Has software running on computers that are connected to or capable of connecting to the Internet been licensed and supported (by the software vendor or supplier of the software) to ensure security patches for known vulnerabilities are made available? **Yes**

- 3) Has out-dated or older software been removed from computers and network devices that are connected to or capable of connecting to the Internet? **Yes**
- 4) Have all security patches for software running on computers and network devices that are connected to or capable of connecting to the Internet been installed within 14 days of release or automatically when they become available from vendors? **Microsoft updates are downloaded by our SCCM server every patch Tuesday and are then tested in a lab environment, depending on the number of updates (and especially with SQL updates) this can sometimes take longer than 14 days but they are always rolled out as soon as testing is complete. Virus Definitions and updates relating to security products are downloaded and installed at least once a day.**
- 5) Are all smart phones kept up to date with vendor updates and application updates? **Yes**
- 6) Are all tablets kept up to date with vendor updates and application updates? **Yes**
- 7) Do you perform regular vulnerability scans of your internal networks and workstations to identify possible problems and ensure they are addressed? **Yes**
- 8) Do you perform regular vulnerability scans of your external network to identify possible problems and ensure they are addressed? **Yes**
- 9) Do all personnel involved with implementing the Cyber Essential Scheme have sufficient knowledge of the scheme to do so effectively? **Yes**
- 10) Could you identify which 3rd party services were in scope of the Cyber Essential Scheme requirements? **Yes**

Abuse of Staff Via Social Media

In a situation where a member of staff is abused (by word and / or image) via social media, the following procedures should be instigated as soon as possible after information has been received:

Same Day Action (there may need to be some flexibility to the following actions, depending on the time at which relevant information is received)

- As soon as information is received, inform Director of Development who will collate evidence and work with IT team to report offence to social media platform. The priority, here, is to have offensive material removed from a public site without losing the evidence.
- Deputy Head and Head of Year to complete immediate investigations with students. This will comprise the writing of statements and one-to-one interviews.
- Girls' iPads and 'phones may be checked to ensure that all material / photographs have been removed permanently from devices.
- Relevant students to work with Director of Development to close / delete accounts if this has not, already, taken place.
- Head and Director of Studies to be informed by Deputy Head as soon as statements are in the process of being written.
- Director of Studies to inform affected staff about the incident at the end of a session (break / lunch / after school). Cover to be provided if necessary.
- The Director of Development to ensure that each member of staff affected is shown what has been posted. Names may be redacted. This should take place as soon as possible after the postings have been identified and certainly within the timing of the school day. Copies of the material should be offered to affected members of staff.
- Secretary to Director of Studies to ensure that students who may be involved are not taught by affected members of staff that day. Director of Studies to consider what the students can do during affected periods.
- Deputy Head to consult with the Head on the action taken so far and discuss sanctions. This may include immediate suspension and removal from school site. Sanctions, (if suspension), should be given swiftly and, unless there is an extraordinary reason not to, should be administered the following school day. (If higher sanctions are to be considered, the Head will follow the Expulsion Policy).
- Deputy Head (or Head – depending on severity of sanctions) to telephone all parents to outline the behaviour and to give information regarding sanctions.
- All affected members of staff to be called to an emergency briefing after school in Head's Office to discuss the action taken so far and support they can access. This meeting should be attended by the Head, Deputy, Director of Studies and Director of Development. Staff should be consulted about the future teaching of those students.
- Letters to be produced and sent to parents, confirming behaviour and actions taken.
- Confidentiality to be maintained as far as possible.

Next Day Action

- Deputy Head and Head should begin seeing parents of those girls who have received serious punishments (unless expulsion policy is being followed).
- Students should be internally suspended / detentions given (if these are the agreed sanctions).

- All affected members of staff called to a further briefing in Head's Office with Deputy and Director of Studies to discuss the situation and any further action needed / concerns. Staff consulted about the future teaching of those students if appropriate.
- Head of Year to support the students as appropriate.

Following Days

- Deputy Head to continue to support staff. Staff to consider restorative justice if appropriate.
- Head of Year to support the students as appropriate.
- Involve school police liaison to talk to students, parents and staff as appropriate.
- Head to consider whole-school response (e.g. Change to policy, key messages given to students).
- Further formal briefing with affected staff, after one week, to consider actions taken and whether any further action is needed.

Alderley Edge School for Girls
POLICY ADDENDUM to Acceptable Use Policy
Pupil Agreement for Online Learning from Home

We are aiming to keep your access to learning and teaching open through a difficult time and staff will be working hard to provide you with lessons via the online systems.

We are asking all pupils to sign an Online Learning Agreement, which is a document that outlines how we expect you to behave when you are learning online.

School systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies. This means anything you do on a school device or using school networks/platforms/internet may be viewed by one of the staff members who are here to keep you safe. You should not behave any differently when you are out of school or using your own device or home network.

The points listed below should be followed at all times and can be summarised as follows:

“Treat yourself and others with respect at all times; treat people in the same way when you are online or on a device as you would face to face.”

What am I agreeing to?

1. I will treat myself and others with respect at all times; when I am online or using a device, I will treat everyone as if I were talking to them face to face in a classroom.
2. 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 school.
3. Even though I am working outside the classroom, I will aim to be positive and creative, to learn and share, to develop new skills and to prepare for the future.
4. I will choose a sensible place to work from – ideally a living room - and I will dress appropriately for my lessons as I would do at school.
5. I will make sure that I have all the tools I need in advance, so that I do not have to leave my desk and interrupt the flow of the lesson.
6. I will be at my lesson on time.

7. I will complete exercises as directed by my teacher and upload completed work to meet the deadlines set by my teacher.
8. I understand that my online lessons will be monitored by senior leaders from the School.
9. I will not under any circumstances provide my login details to anyone else. The system is fully secured and my activity on the system can be monitored.
10. I can share work with other pupils in my class but I should let my teacher know who else I am working with.
11. I understand that websites, blogs, videos and other online information can be biased and misleading, so I will need to check sources.
12. I will not download copyright-protected material (text, music, video etc.), and I will avoid plagiarism.
13. I will not browse, download, upload, post, share or forward material that could be considered offensive, harmful or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
14. 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.
15. I will not share my or others' personal information that can be used to identify me, other students or my teachers on any online space, unless a trusted adult has given permission or reviewed the site.
16. I will never take secret photos, recordings or videos of teachers or other students.
17. I will never say, text or post anything that could hurt or embarrass another person. I will never use the internet to bully anyone.
18. I will join the lessons at the times I have been given and if I am unable to join the session for any reason e.g. through ill health, I will let my teacher know in advance.

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

**Signed:** \_\_\_\_\_

**Date:** \_\_\_\_\_

**Appendix – Staff Agreement for Online Teaching from Home**

## **Alderley Edge School for Girls** **Staff Protocol for Online Teaching from Home**

We ask all staff at Alderley Edge School for Girls to read and carefully review this Online Learning Agreement. It is an addendum to the existing Acceptable Use Policies and procedures in place for use of the Internet and of ICT. This is a document that outlines how we expect you to conduct yourself when you are teaching remotely. Please be aware that Senior Leaders will maintain oversight of lessons held remotely through regular monitoring.

### **Safety First**

**Key e-safety messages and understanding should be reinforced as part of each lesson.**

- Staff should reinforce e-safety messages during lessons and when setting homework that requires access to the internet. This includes access to messaging systems (such as Teams, Office 365), internet notice boards, and other internet based educational resource environments.
- Students should be encouraged to be critically aware of the content they access on-line and be guided to validate the accuracy of information.
- Students should also be taught to acknowledge the source of information used – never to plagiarise - and to respect copyright when using material accessed on the internet.
- Bullying is an unfortunate feature of the online environment and the perceived anonymity can add to this. Staff should be alert to pupils working in groups online where suddenly the relationships seem to break down.
- If staff feel that the system is not being used appropriately – the same protocols exist as if the school were functioning normally. The DSL has the same responsibilities for safeguarding and should be the first port of call for any concerns about the online safety of our pupils.
- Behavioural issues should be dealt with in line with the school's Behaviour Policy and sanctions can be applied that will come into effect once the school is back in operation on site.

## Code of Conduct

- Always behave appropriately online as you would do in the classroom, ensuring that your standards of dress match the standards expected in school.
- Set appropriate boundaries and maintain the same professional standards as you would at school. Online working should not lead to a relaxation in staff student protocols.
- Never make inappropriate jokes or comments online.
- Any digital communication between staff and pupils, or parents and guardians should be professional in tone and content.
- Contact with pupils should only be through school email accounts, Microsoft Team or other School approved educational platforms. Other methods of contact such as phones, private email or social media accounts should not be used under any circumstances.
- Never follow or interact with pupils on your personal social media account.

## Choosing a venue

- Choose a suitable venue for conducting the lesson. This should never be a bedroom or personal space.
- Make sure that it is a quiet space, with no ambient noise, and friends and family are never visible during a lesson.
- Always check what is visible on screen to the pupil - avoid including inappropriate personal items, paintings/posters etc.
- Make sure there is never a possibility of strangers having access to your screen.

## Staff Responsibilities

- **Subject Teachers** are responsible for offering guidance and support to their pupils on how to manage their online learning and for referring pupils to the appropriate sources of academic or welfare advice when necessary.
- Staff will be expected to have knowledge of the individual pupil's programme of study, keeping that pupil up to date with expectations of delivery and assessment and to be proactive in communicating with the pupils in their subject area. Teachers will also be expected to monitor collaborative work where pupils are asked to work together to solve a problem or develop a project.

- **SLT** are responsible for ensuring the online tutoring of pupils in their subject areas is in line with this addendum to the Code of Practice.
- SLT will check the usage logs to ensure that lessons are taking place at the appropriate times if required.
- **Students** are responsible for attending online sessions with teachers, for being adequately prepared for online lessons, and for communicating with the online teacher if for any reason they are unable to attend these sessions.
- **Tutors** are responsible for ensuring that all pupils are logging in to online activity, are present during their online lessons and meet the expectations for attendance as if they were in school.

## Conducting the Lesson

- Make sure your equipment and materials are organized in advance of your lesson. Be well prepared.
- Be strict about class times and stick to them.
- Maintain your presence as you would in class.
- Give clear instructions. Clear lesson plans are advisable so that you can cover the focus areas within the timeframe.
- Set homework as you would at school and ensure it is uploaded to ShowMyHomework, and make sure this is marked. Give written feedback, and oral feedback in the lesson.
- Do not interrupt lessons to search for refreshments. Do not eat snacks or meals during lessons.
- Through sickness, absence or the nature of your teaching responsibilities there may be a possibility that you work with only one pupil at a time. Please treat this eventuality exactly as you would at school.

## Data Protection

- Under GDPR all online content from a pupil could be regarded as personal data and is subject to the provisions under the Data Protection Act.
- The names, emails and phone numbers of students are personal data. This means that only relevant people should have access, and the information should only be kept as long as it is required.

- Personal data should only be used to assist you to carry out your work. It must not be given out to people who have no right to see it.
- All staff should maintain the security of all computerized databases of information on individuals, whether they are staff, pupils or members of the general public. Any queries in this regard should be referred to the Headteacher.
- Pupils have been asked to give their permission (by signing a separate agreement) for their data to be used on a temporary basis i.e. during their absence from school as a result of the Covid-19 school closures.

Please note that:

- All Student data should be viewed via 3SYS directly, no student data should be downloaded to a private device or printed off.
- Data should only be accessible to those staff that need it. (For example, science teachers should only have information for their own class groups, not every student in the whole year group.)
- The information should be deleted after it has been used for this purpose.

~~~~~

I have read and understand the above requirements and agree to follow them.

Signed: _____

Date: _____

NOTES ON THE USE OF MICROSOFT TEAMS

Microsoft Teams is a closed system for those of us using it under the school’s Microsoft licence but it is a powerful piece of software with a number of collaborative tools and staff should be alert to the fact that pupils may well have better mastery of it than themselves. For example, Teams provides a facility for pupils to set up their own groups.

There is end to end encryption contained in the software and this can be enabled which means that “chats” can be private for groups/users.

All calls and group chats/videos can be recorded and it is recommended that all lessons are recorded especially where staff are conducting a one to one session.

If there are difficulties with the connections for staff or the pupil the lesson should be suspended, the issue reported to the IT team and the “lesson” resumed once the connection problems have been solved.

Alderley Edge School for Girls – Prep School Reception to Year 6: POLICY ADDENDUM

Pupil Agreement for Online Learning from Home

We are aiming to keep your access to learning and teaching open through a difficult time and staff will be working hard to provide you with lessons via the online systems. We are asking all pupils to sign an Online Learning Agreement, which is a document that outlines how we expect you to behave when you are learning online.

School systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies. This means anything you do on a school device or using school networks/platforms/internet may be viewed by one of the staff members who are here to keep you safe.

You should not behave any differently when you are out of school or using your own device or home network.

The points listed below should be followed at all times and can be summarised as follows: “Treat yourself and others with respect at all times; treat people in the same way when you are online or on a device as you would face to face.”

What am I agreeing to?

1. I will treat myself and others with respect at all times; when I am online or using a device, I will treat everyone as if I were talking to them face to face in a classroom.
2. 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 school.
3. Even though I am working outside the classroom, I will aim to be positive and creative, to learn and share, to develop new skills and to prepare for the future.
4. I will choose a sensible place to work from – ideally a kitchen or living room - and I will dress appropriately for my lessons as I would do at school.
5. I will make sure that I have everything I need for a lesson, so I don't need to leave part way through, interrupting the flow of the lesson.
6. I will be at my lesson on time.
7. I will complete exercises as directed by my teacher and upload completed work to meet the deadlines set by my teacher.
8. I understand that my online lessons will be monitored by senior leaders from the School.

9. I will not under any circumstances provide my login details to anyone else. The system is fully secured and my activity on the system can be monitored.
10. I can share work with other pupils in my class but I should let my teacher know who else I am working with.
11. I understand that websites, blogs, videos and other online information can be biased and misleading, so I will need to check sources.
12. I will not download copyright-protected material (text, music, video etc.).
13. I will not browse, download, upload, post, share or forward material that could be considered offensive, harmful or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
14. 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.
15. I will not share my or others' personal information that can be used to identify me, other students or my teachers on any online space, unless a trusted adult has given permission or reviewed the site.
16. I will never take secret photos, recordings or videos of teachers or other students.
17. I will never say, text or post anything that could hurt, embarrass or isolate another person. I will never use the internet to bully anyone. Bullying will be dealt with immediately and in line with school policy.
19. I will join the lessons at the times I have been given and if I am unable to join the session for any reason e.g. through ill health, I will let my teacher know in advance.

I have read and understand these rules and agree to them. Signed (pupil):
_____ Date: _____