



Brewood and Wheaton Aston Federation
POLICY STATEMENT

Online Safety Policy

*We value and cherish every member of our community and celebrate their uniqueness.
Our values led curriculum promotes a love of life and learning inspiring every individual to be a respectful,
resilient, and faithful global citizen.*

*"Let all that you do be done in love."
1 Corinthians 16:14*

Respect, Faith, Resilience

Signed: L. Ray Chair of LAC Date: **2 MAY 2025**

Signed: Chair of LAC Date:

Signed: Chair of LAC Date:

Signed: Chair of LAC Date:

Reviewed: Jan 2025

Review Date: Jan 2026

- **Development, monitoring and review of the Policy**
- **Schedule for development, monitoring and review**
- **Scope of the Policy**
- **Roles and Responsibilities**
 - Local Academy Committee
 - Principal and Senior Leaders
 - Online Safety Coordinator
 - Network Manager
 - Teaching and Support
 - Child Protection / Safeguarding Designated Person / Officer
 - Pupils
 - Parents / Carers
 - Community Users
- **Staff Policy Statements**
 - Education – Pupils
 - Education – Parents / Carers
 - Education – The Wider Community
 - Education and training – Staff / Volunteers
 - Training – Local Academy Committee
 - Technical – infrastructure / equipment, filtering and monitoring
 - Bring your own devices (BYOD)
 - Use of digital and video images
 - Data protection
 - Communications
 - Social Media - Protecting Professional Identity
 - User Actions - unsuitable / inappropriate activities
 - Responding to incidents of misuse

Development / Monitoring / Review of this Policy

This Online safety policy has been developed by:

- *Head of Computing – Mr James Dean*
- *Head of School – Mr J Smith*

Consultation with the school community has taken place through a range of formal and informal meetings with

- *Exec Principal – Mr R Dickson*
- *Head of School – Mr J Smith*
- *LAC member of safeguarding – Mrs S Bradley-Richards*

Schedule for Development / Monitoring / Review

This online safety policy was approved by the Local Academy Committee on:	<i>March 2025</i>
The implementation of this Online safety policy will be monitored by the:	<i>SLT / LAC members</i>
Monitoring will take place at regular intervals:	<i>September. Each year starting from 2017</i>
The LAC will receive a report on the implementation of the Online safety policy generated by the monitoring group (which will include anonymous details of Online safety incidents) at regular intervals:	<i>Termly meetings</i>
The Online safety Policy will be reviewed annually, 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:	<i>January</i>
Should serious Online safety incidents take place, the following external persons / agencies should be informed:	<i>Exec Principal / Head of School, then SCAS - safeguarding contacted.</i>

The academy will monitor the impact of the policy using:

- *SIMS Behaviour logs*
- *SENSO Monitor Monitoring Sheet (Weekly check by Mr James Dean)*
- *SENSO Monitor Software on the network*

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Principals to such extent as is reasonable, to regulate the behaviour of pupils when they are off the academy 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 academy, but is linked to membership of the academy.

The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The academy will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

The Academy's own use of social media is guided by the principles of the Church of England's Social Media Charter:

"Social media is a very public way of enabling us as Christians to live out our calling to share the good news of Jesus Christ. One of its many joys is that it is immediate, interactive, conversational and open-ended. This opportunity comes with a number of downsides if users do not apply the same common sense, kindness and sound judgement that we would use in a face-to-face encounter. While written specifically for all users who engage with the Church of England's and Archbishops' national social media channels, these guidelines are built on universal principles."

The Academy seeks to promote the following:

- **Be safe.** The safety of children, young people and vulnerable adults must be maintained.
- **Be respectful.** Do not post or share content that is sexually explicit, inflammatory, hateful, abusive, threatening or otherwise disrespectful.
- **Be kind.** Treat others how you would wish to be treated and assume the best in people. If you have a criticism or critique to make, consider not just whether you would say it in person, but the tone you would use.
- **Be honest.** Don't mislead people about who you are.
- **Take responsibility.** You are accountable for the things you do, say and write. Text and images shared can be public and permanent, even with privacy settings in place. If you're not sure, don't post it.
- **Be a good ambassador.** Personal and professional life can easily become blurred online so think before you post.
- **Disagree well.** Some conversations can be places of robust disagreement and it's important we apply our values in the way we express them.
- **Credit others.** Acknowledge the work of others. Respect copyright and always credit where it is due. Be careful not to release sensitive or confidential information and always question the source of any content you are considering amplifying.
- **Follow the rules.** Abide by the terms and conditions of the various social media platforms themselves. If you see a comment that you believe breaks their policies, then please report it to the respective company.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the academy:

Local Academy Committee (LAC):

The LAC 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 Local Academy Committee (LAC) receiving regular information about Online safety incidents and monitoring reports. Mrs Sue Bradley Richards has taken on the role of online safety LAC Link. The role of the online safety LAC Link will include:

- meetings with Online Safety Lead Mr James Dean
- SIMS Behaviour logs.
- regular monitoring of SENSO incident monitoring logs.
- reporting to relevant LAC members

Executive Principal and Senior Leaders:

- The Exec Principal has a duty of care for ensuring the safety (including online safety) of members of the academy's community, though the day-to-day responsibility for online safety will be delegated to the Head of Computing.
- The Exec Principal and Head of School 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. SWGfL BOOST includes an 'Incident Response Tool' that steps (and forms to complete) any staff facing an issue, disclosure or report, need to follow. This can be downloaded at [http://www.swgfl.org.uk/Staying-Safe/Online safety-BOOST/Boost-landing- page/Boost-Hub/Incident-Response-Tool](http://www.swgfl.org.uk/Staying-Safe/Online%20safety-BOOST/Boost-landing-page/Boost-Hub/Incident-Response-Tool)
- The Exec Principal and Head of School are responsible for ensuring that the Head of Computing 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 Exec Principal and Head of School will ensure that there is a system in place to allow for monitoring and support of those in at the academy 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 Principal will review logs February and September annually.
- The Senior Leadership Team will receive regular monitoring reports from the Head of Computing.

Online safety Coordinator: Head of Computing – Mr J Dean

- takes day to day responsibility for Online safety issues and has a leading role in establishing and reviewing the academy's 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 Local Authority.
- liaises with the academy's 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 Link Governor to discuss current issues and review incident logs.
- reports regularly to Senior Leadership Team.

Network Managers: Concerro

The Network Manager is responsible for ensuring:

- that the academy's technical infrastructure is secure and is not open to misuse or malicious attack
- that the academy meets required online safety technical requirements and any Local Authority guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed (KS2 pupil have the same password till KS3, KS3 pupils can change theirs on each access).
- the filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- 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 / Office 365/ remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Head of School /SLT / Online safety Coordinator for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in academy policies

Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current academy Online safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the Exec Principal / Senior Leader / Online safety Coordinator for investigation / action / sanction
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official academy 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 academy 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

Safeguarding Designated Person: Head of School – Mr J Smith

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

Pupils:

- are responsible for using the academy digital technology systems in accordance with the Pupil Acceptable Use 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 academy's Online safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

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

- digital and video images taken at academy events.
- their children's personal devices in the academy (where this is allowed)

Community Users

Community Users who access academy systems / website / Office 365 as part of the wider *academy* provision will be expected to sign a Community User AUP before being provided with access to academy systems.

These users will have limited access to academy systems and be monitored by SENSO MONITOR software.

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 academy's online safety provision. Children and young people need the help and support of the academy 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 should be provided as part of Computing and PHSE (LIFE) and should be regularly revisited.
- Key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities.
- Pupils should 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 should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside the academy.
- Staff should 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 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.
- Where pupils are allowed to freely search the internet, staff should 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, should be auditable, with clear reasons for the need.

Education – parents / carers

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 online 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 academy will therefore seek to provide information and awareness to parents and carers through:

- Entrust parental online safety training sessions.
- Curriculum activities
- Social media
- Letters
- Annual CCA Online safety Week
- Reference to the relevant web sites / publications e.g. www.thinkuknow.com
www.swgfl.org.uk www.saferinternet.org.uk/ <http://www.childnet.com/parents-and-carers>

Education – The Wider Community

The academy will provide opportunities for local members of the community to gain from the academy's online safety knowledge and experience. This will be offered through the following:

- Online safety messages from the school through updates, Head of School newsletter, National Online Safety guides sent out to parents

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 training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the academy online safety policy and Acceptable Use Agreements.
- The online safety Coordinator will receive regular updates through attendance at external training events (e.g. from Entrust) 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 meetings and INSET days.
- The Head of Computing will provide advice and training to individuals as required.

Training – LAC members

Local Committee members should take part in Online safety training / awareness sessions, with particular importance for those responsible for child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority.
- Participation in school training / information sessions for staff or parents.

Technical – equipment, filtering and monitoring

The academy will be responsible for ensuring that the academy's 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:

- Academy technical systems will be managed in ways that ensure that the academy meets recommended technical requirements
- **There** will be regular reviews and audits of the safety and security of academy's technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to academy technical systems and devices.
- All users will be provided with a username and secure password by their computing teacher who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password every year.

- The administrator passwords for the academy ICT system, used by the Network Manager (or other person) must also be available to the Exec Principal or other nominated senior leader and kept in a secure place (e.g. school safe)
- CONCERO are 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 broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.
- Academy technical staff regularly monitor and record the activity of users on the academy's technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the teacher or Head of Computing.
- 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 academy's systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date 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 academy's systems. Trainee and temporary staff will be given a username to access the staff drive for lesson resources.
- An agreed policy is in place regarding the extent of personal use that users (staff / pupils / community users) and their family members are allowed on academy devices that may be used out of the academy. Staff devices are monitored by SENSO Monitor software when used outside of the academy. Online behaviour using these devices must therefore be appropriate to the academy's expectations.
- An agreed policy is in place that allows staff to / forbids staff from downloading executable files and installing programmes on academy devices. Any staff who intentionally place malicious software on academy devices would face disciplinary action.
- Removable media (e.g. memory sticks / CDs / DVDs) can be used appropriately by users on academy devices. Personal data cannot be sent over the internet or taken off the academy's site unless safely encrypted or otherwise secured.

Use of digital and video images

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 academy 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 / carers are welcome to take videos and digital images of their children at academy events for their own personal use (as such use is 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 / carers comment on any activities involving other pupils in the digital / video images.

- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on academy 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 academy into disrepute.
- 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.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the academy's website.

Data Protection

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 academy 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 is registered as a Data Controller for the purposes of the Data Protection Act (DPA).
- Responsible persons are Exec Principal and Mrs S Cornes
- Risk assessments are carried out on a case by case basis.
- 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 be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with the academy's policy (below) once it has been transferred or its use is complete.

Communications

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

		Staff & other adults			Pupils				
	Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
	Mobile phones may be brought to the academy								
	Use of mobile phones in lessons								
	Use of mobile phones in social time								
	Taking photos on mobile phones / cameras								
	Use of other mobile devices e.g. tablets, gaming devices								
	Use of personal email addresses at the academy or on academy's network								
	Use of academy email for personal emails								
	Use of messaging apps								

	Use of social								
	Use of blogs								

When using communication technologies the academy considers the following as good practice:

- The official academy email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Pupils should therefore use only the academy email service to communicate with others when in academy, or on academy systems (e.g., by remote access).
- Users must immediately report, to the nominated person – in accordance with the academy 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 / carers (email, chat, Office 365 etc.) must be professional in tone and content. These communications may only take place on official (monitored) academy systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils will be provided with individual academy email addresses for educational use.
- Pupils should 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 academy website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies 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 academy or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The academy 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

Academy staff should ensure that:

- No reference should be made in social media to pupils, parents / carers or academy staff.
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the academy or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The academy's use of social media for professional purposes will be checked regularly by the senior risk officer to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Unsuitable / inappropriate activities

The academy believes that the activities referred to in the following section would be inappropriate in a academy context and that users, as defined below, should not engage in these activities in the academy or outside of the academy when using academy equipment or systems. The academy policy restricts usage as follows:

User Actions

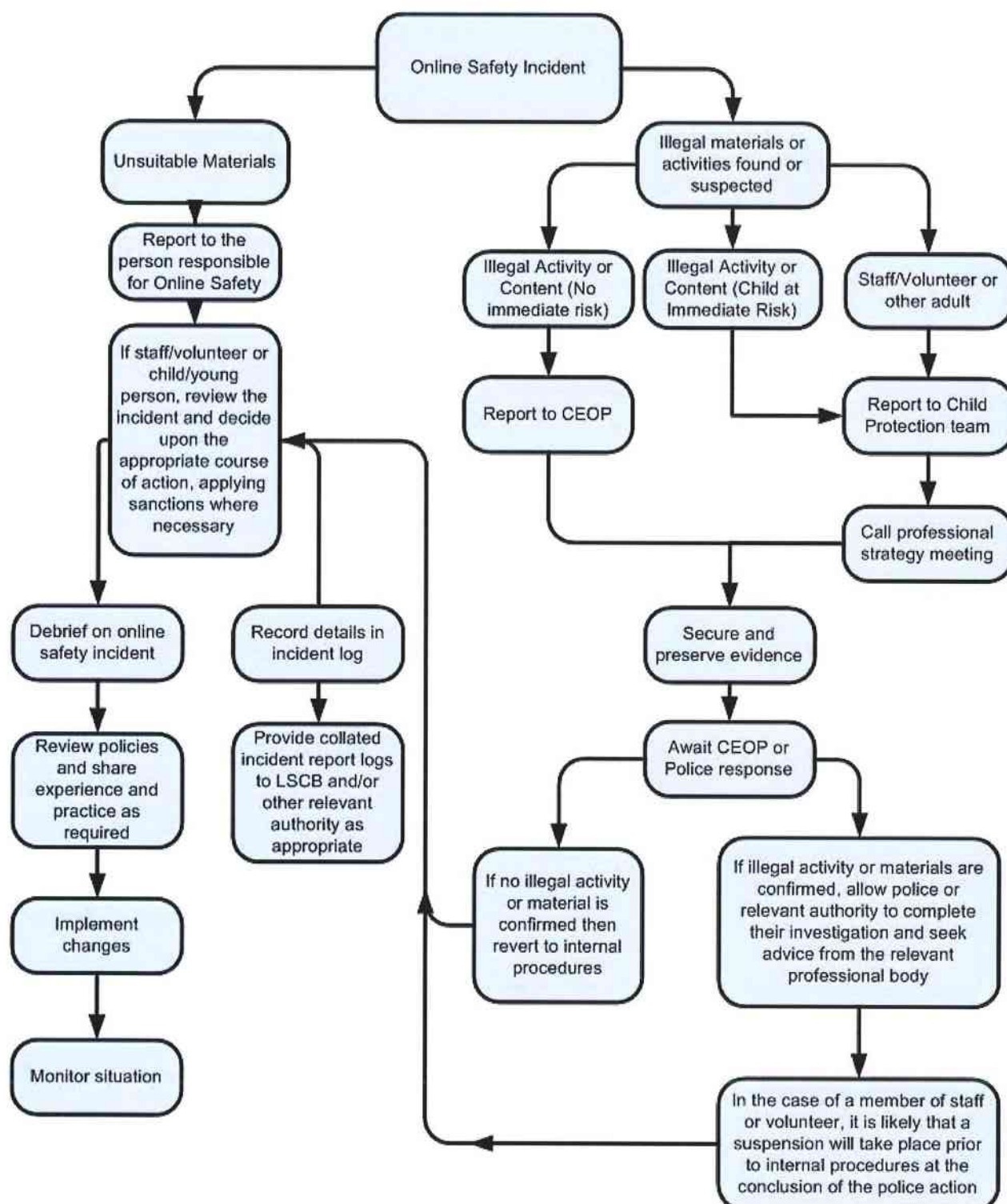
		Acceptable	Acceptable at certain	Acceptable for nominated	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)		X				
On-line gaming (non-educational)				X		
On-line gambling					X	
On-line shopping / commerce				X		
File sharing				X		
Use of social media					X	
Use of messaging apps					X	
Use of video broadcasting e.g. YouTube		X				

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 (see "User Actions" above).

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 for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the academy community will be responsible users of digital technologies, who understand and follow academy 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 Local Authority 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 *academy* 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.

Academy Actions & Sanctions

It is more likely that the academy 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 academy 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 as follows:

Pupils

Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / SLT	Refer to Exec Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X			X		X
Unauthorised use of non-educational sites during lessons	X								
Unauthorised use of mobile phone / digital camera / other mobile device	X	X							
Unauthorised use of social media / messaging apps / personal email	X				X		X		X
Unauthorised downloading or uploading of files	X				X			X	
Allowing others to access academy network by sharing username and passwords	X							X	
Attempting to access or accessing the academy network, using another student's / pupil's account	X							X	
Attempting to access or accessing the academy network, using the account of a member of staff	X	X			X	X	X		X
Corrupting or destroying the data of other users	X	X			X	X			X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X			X	X			X
Continued infringements of the above, following previous warnings or sanctions	X	X			X	X	X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X		X	X	X		X
Using proxy sites or other means to subvert the school's / academy's filtering system	X	X	X		X	X	X		X
Accidentally accessing offensive or pornographic material and failing to report the incident	X							X	
Deliberately accessing or trying to access offensive or pornographic material	X	X			X	X	X		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X			X	X			X

Staff

Actions / Sanctions

Incidents:	Refer to line manager	Refer to Exec.Principal	Refer to SCAT / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X	X	X	X			X
Inappropriate personal use of the internet / social media / personal email	X	X				X		
Unauthorised downloading or uploading of files	X	X				X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X	X				X		
Careless use of personal data e.g. holding or transferring data in an insecure manner	X	X				X		
Deliberate actions to breach data protection or network security rules	X	X	X		X			X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X	X		X			X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X		X			X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils	X	X	X		X			X
Actions which could compromise the staff member's professional standing	X	X			X	X		
Actions which could bring the academy into disrepute or breach the integrity of the ethos of the academy	X	X			X	X		
Using proxy sites or other means to subvert the school's / academy's filtering system	X	X			X	X		
Accidentally accessing offensive or pornographic material and failing to report the incident					X			
Deliberately accessing or trying to access offensive or pornographic material		X	X		X			X
Breaching copyright or licensing regulations	X	X			X			X
Continued infringements of the above, following previous warnings or sanctions	X	X	X		X			X

Pupil Acceptable Use Agreement

Academy Policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside the academy. These 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. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The academy will try to ensure that *pupils* will have good access to digital technologies to enhance their learning and will, in return, expect the *pupils* to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use academy 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.

For my own personal safety:

- I understand that the academy will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, 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 be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the *academy* systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make 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 use the *academy* systems or devices for on-line gaming, on-line gambling, internet shopping or file sharing unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the academy has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the academy:

- I will only use my own personal devices (mobile phones / USB devices etc.) in the academy if I have permission. I understand that, if I do use my own devices in the academy, I will follow the rules set out in this agreement, in the same way as if I was using academy equipment.

- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I 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 immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, 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 not install or attempt to install or store programmes of any type on any academy device, nor will I try to alter computer settings.
- I will not use social media on the academy network.

When using the internet for research or recreation, I recognise that:

- I should 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 try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of the academy:

- I understand that the *academy* also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of the academy and where they involve my membership of the academy community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the academy network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to academy systems and devices.

Pupil Acceptable Use Agreement Form

Responsible Internet Use

The computer system is owned by the academy. This responsible Internet Use statement helps to protect pupils by clearly stating what use of the computer resources is acceptable and what is not.

- I will only use my own network login and password which will be kept secret
- I will only look at and delete my own files
- I understand that I must not bring software into the academy without permission.
- I am responsible for e-mail/ Office messages that I send and for contacts made. I will only send messages which are polite, sensible and free from unsuitable language. I will ensure that they are carefully written. I will not send any attachments which are hurtful, abusive or offensive.
- If I receive anything, see anything or come across a website which may be unsuitable for any member of our academy, then I will tell my teacher, tutor or ICT technician immediately.
- I understand that I must never give my home address, phone number, send photos, give out personal information, or arrange to meet someone who contacts me over the internet.
- I will not send anonymous messages and I know that fake account profiles are not permitted.
- I will not use social media or chat facilities online.
- I will respect the security of the ICT system; it is a criminal offence to use a computer for a purpose not permitted by the system owner.
- I know that any information I copy from the internet and use in my work, is not my own work. I will acknowledge that it is not all my own work and where I have got this information from.
- I understand that if I deliberately break these rules, I will not be allowed to use the internet and/or e-mail and that my parents will be informed.

The academy will exercise its right to monitor the use of the academy's computer systems. This will include access to websites, the interception of e-mail and the deletion of inappropriate material where it believes unauthorised use of the academy's computer system is or may be taking place, or the system is or may be being used for a criminal purpose or for storing unauthorised or unlawful text, images, video or sound.

Signed (Pupil)

Signed (Parent/Carer)

Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of the academy. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the website and occasionally in the public media,

The academy will comply with the Data Protection Act and request parents / carers permission before taking images of members of the academy. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at academy events for their own personal use (as such use is 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 / carers comment on any activities involving other *pupils* in the digital / video images.

Parents / carers are requested to sign a permission form to allow the academy to take and use images of their children for specific uses and for the parents / carers to agree.

Appendices

1. Pupil Acceptable Use Policy – Key Stage 2 & Key Stage 3
2. Staff Acceptable Use Policy
3. Parent Acceptable Use Policy
4. Visitors / Volunteers Acceptable Use Policy
5. Supply Staff Acceptable Use Policy
6. Access to Electronic Mail and the Internet
7. Mobile Phone policy
8. Academy Technical Security
9. Other documents
10. Legislation
11. Links to other organisations and documents
12. Resources



Appendix 1

Acceptable Use Policy (AUP) for KS2 PUPILS



These statements can keep me and others safe & happy at the academy and home

1. ***I learn online*** – I use the academy's internet, devices and logons for school work, homework and other activities to learn and have fun. All academy devices and systems are monitored, including when I'm using them at home.
2. ***I learn even when I can't go to school because of coronavirus*** – I don't behave differently when I'm learning at home, so I don't say or do things I wouldn't do in the classroom or nor do teachers or tutors. If I get asked or told to do anything that I would find strange in school, I will tell another teacher.
3. ***I ask permission*** – At home or school, I only use the devices, apps, sites and games I am allowed to and when I am allowed to.
4. ***I am creative online*** – I don't just spend time on apps, sites and games looking at things from other people. I get creative to learn and make things.
5. ***I am a friend online*** – I won't share or say anything that I know would upset another person or they wouldn't want shared. If a friend is worried or needs help, I remind them to talk to an adult, or even do it for them.
6. ***I am a secure online learner*** – I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords!
7. ***I am careful what I click on*** – I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes app add-ons can cost money, so it is important I always check.
8. ***I ask for help if I am scared or worried*** – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
9. ***I know it's not my fault if I see or someone sends me something bad*** – I won't get in trouble, but I mustn't share it. Instead, I will tell a trusted adult. If I make a mistake, I don't try to hide it but ask for help.
10. ***I communicate and collaborate online*** – with people I already know and have met in real life or that a trusted adult knows about.
11. ***I know new online friends might not be who they say they are*** – I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are.
12. ***I check with a parent/carer before I meet an online friend*** the first time; I never go alone.
13. ***I don't do live videos (livestreams) on my own*** – and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the first time.
14. ***I keep my body to myself online*** – I never get changed or show what's under my clothes when using a device with a camera. I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.

15. ***I say no online if I need to*** – I don't have to do something just because someone dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.
16. ***I tell my parents/carers what I do online*** – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.
17. ***I follow age rules*** – 13+ games and apps aren't good for me so I don't use them – they may be scary, violent or unsuitable. 18+ games are not more difficult or skills but very unsuitable.
18. ***I am private online*** – I only give out private information if a trusted adult says it's okay. This might be my address, phone number, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again.
19. ***I am careful what I share and protect my online reputation*** – I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).
20. ***I am a rule-follower online*** – I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, block bullies and report bad behaviour, at home and at school.
21. ***I am not a bully*** – I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.
22. ***I am part of a community*** – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult and/or report it.
23. ***I respect people's work*** – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons license.
24. ***I am a researcher online*** – I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, know which sites to trust, and know how to double check information I find. If I am not sure I ask a trusted adult.

~~~~~

**I have read and understood this agreement.**

**If I have any questions, I will speak to a trusted adult: at school that includes my class teacher, Teaching Assistants and Senior Leadership Team**

**Outside school, my trusted adults are \_\_\_\_\_**

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

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

## For parents/carers

If your parents/carers want to find out more, they can read Brewwood's full Online Safety Policy <http://www.brewwood.staffs.sch.uk/wp-content/uploads/bsk-pdf-manager/2020/09/BMA-e-safety-Policy.pdf> for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding Policy, Behaviour Policy, etc). They will also have been asked to sign an AUP for parents.



## Acceptable Use Policy (AUP) for **KS3 PUPILS**

### What am I agreeing to?

1. I will treat myself and others with respect at all times; when I am online or using any device, I will treat everyone as if I were talking to them face to face.
2. Whenever I use a device, the internet or any apps, sites and games, I will try to be positive and creative, to learn and share, to develop new skills, to have fun and prepare for the future.
3. I consider my online reputation with everything that I post or share – I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).
4. I will tell a trusted adult if I have a problem or am worried about something online, and I will encourage my friends to do so too. Statistics show that telling someone helps!
5. It can be hard to stop using technology sometimes, for young people and adults. When my parents/carers or teachers talk to me about this, I will be open and honest if I am struggling.
6. It is not my fault if I stumble across (or somebody sends me) something violent, sexual or otherwise worrying. But I will not share or forward it, and I will ask a trusted adult for advice/help.
7. If I see anything that shows people hurting themselves or encouraging others to do so, I will report it on the app, site or game and tell a trusted adult straight away.
8. I will ensure that my online activity or use of mobile technology, in school or outside, will not cause my school, the staff, students or others distress or bring the academy into disrepute.
9. I will only use the academy's internet, systems, devices and logins for academy-related activities for activities that are appropriate to what I am doing at that time (e.g., at school I don't play games unless I am allowed to, e.g. during lunch, and at home I don't access inappropriate sites or apps).
10. Whenever I use the internet or devices in school **OR use academy devices at home OR log in on home devices at home**, I may be monitored or filtered; the same behaviour rules always apply.
11. I will keep logins, IDs and passwords secret and change my password regularly. If I think someone knows one of my passwords, I will change it; if I think they have used it, I will tell a teacher.
12. I will not try to bypass academy security in any way or access any hacking files or tools.
13. I will only edit or delete my own files and not (even try to) view, change or delete other people's files or user areas without their permission.
14. I will use the internet, apps, sites & games responsibly; I will not use any that are inappropriate for school use or for my age, including sites which encourage hate or discrimination.
15. I understand that any information I see online could be biased and misleading, so I should always check sources before sharing (see [fakenews.lgfl.net](https://fakenews.lgfl.net) for support).
16. I understand that bullying online or using technology is just as unacceptable as any other type of bullying, and will not use technology to bully, impersonate, harass, threaten, make fun of or upset anyone, at school or outside. I will stand up for my friends and not be a bystander.
17. I will not post, look at, up/download or share material that could be offensive, harmful or illegal. If I come across any, I will report it immediately.
18. I know some sites, games and apps have age restrictions (most social media are 13+) and I should respect this. 18-rated games are not more difficult but inappropriate for young people.
19. When I am at school, I will only message or mail people if it's relevant to my learning.
20. 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.





21. I will be careful when opening files and attachments, checking for viruses etc. If I am unsure I will not open a file, hyperlink or any other attachment.
22. I will not download copyright-protected material (text, music, video etc.).
23. I will not share my or others' personal information that can be used to identify me, my family or my friends on any online space, unless a trusted adult has given permission or reviewed the site.
24. Livestreaming can be fun, but I always check my privacy settings and know who can see what and when. If I livestream, my parents/carers know about it.
25. I know new online friends might not be who they say they are, so I am always very careful when someone wants to 'friend' me. Unless I have met them face to face, I can't be sure who they are.
26. I will never arrange to meet someone face to face who I have only previously met in an app, site or game without telling and taking a trusted adult with me.
27. **When learning remotely, teachers and tutors will not behave any differently** to when we are in school. If I get asked or told anything that I would find strange in school, I will tell another teacher.
28. I will only use my personal devices (mobiles, smartwatches etc) in school if I have been given permission, and I will never take secret photos, videos or recordings of teachers or students, **including when learning remotely.**
29. I will respect my body and other people's – part of that means using positive words about myself and others; it also means not revealing too much on camera and not sharing or posting photos or videos that show me or anyone else without all my/their clothes on.
30. Many apps can identify where I am or where I made a post or took a photo, so I know how to turn off location settings so everyone doesn't see where I am, where I live or go to school.
31. What I do on devices should never upset or hurt others & I shouldn't put myself or others at risk.
32. If I see, watch, read, hear or receive anything I am unhappy with or I receive a message that makes me feel uncomfortable, e.g. bullying, sexual, extremist/hateful content, I will not respond to it but I will talk to a trusted adult about it.
33. I don't have to keep a secret or do a dare or challenge just because someone (even a friend) tells me to – real friends don't put you under pressure to do things you don't want to.
34. It is illegal to view any form of pornography if you are under 18 years old; I will not attempt to do so and will report anyone who tries to trick me into doing so.
35. I can always say no online, end a chat or block someone; if I do, it's best to talk to someone, too.
36. I know who my trusted adults are at school, home and elsewhere, but if I know I can also get in touch with [Childline](#), [CEOP](#) or [The Samaritans](#).

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

Signed: _____

Date: _____

Appendix 2



Brewwood CE Middle Academy

Staff Acceptable Use Policy Agreement Jan 2025



New technologies have become integral to the lives of children and young people in today's society, both within schools / academies 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 access to the internet and digital technologies 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 / academy 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 technology in their everyday work.

The academy will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for *students / pupils* learning and will, in return, expect staff and volunteers to agree to be responsible users.

Staff and pupils will be asked to agree to follow the acceptable use policies each time they log on to the computer.

Acceptable Use Policy Agreement

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

For my professional and personal safety:

- I understand that the *school / academy* will monitor my use of the academy digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the academy digital technology 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 immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using *school / academy* 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 academy'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 academy website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only communicate with students / pupils and parents / carers using official academy systems. Any such communication will be professional in tone and manner. I will not engage in any on-line activity that may compromise my professional responsibilities.

The academy and the Multi Academy Trust have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the academy:

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using academy equipment. I will also follow any additional rules set by the academy 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 use personal email addresses on the academy ICT systems.
- 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 that my data is regularly backed up.
- 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 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 / academy policies.
- I will not disable or cause any damage to school / academy 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 School / Academy / LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted / password protected. Paper based Protected and restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student / 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 / academy 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.

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

- I understand that this Acceptable Use Policy applies not only to my work and use of school / academy digital technology equipment in the academy, but also applies to my use of school / academy systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the academy.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Local Academy Committee and in the event of illegal activities the involvement of the police.

Communications:

Actions in school time:	Allowed	Allowed at certain times	Not allowed
Mobile phones may be brought into the academy	✓		
Use of personal mobile phones in lesson time			✓
Use of personal mobile phones in social time (in accordance with the academy's Staff Conduct & Behaviour policy) *	✓		
Taking photographs of pupils on mobile phones			✓
Taking photographs on other academy camera devices	✓		
Use of hand held devices e.g. PDA's, school i-pads, tablets in lesson time		✓	
Accessing personal email addresses whilst in school using the academy's network			✓
Use of academy email address for personal e-mails / communication		✓	
Use of chatrooms / social networking whilst in school			✓
Use of instant messaging whilst in lessons			✓
Use of instant messaging whilst in school (in accordance with the academy's staff behaviour policy)		✓	
Use of personal blogs			✓

*Mobile phones and personally-owned devices may not be used during lessons or formal school time. They should be switched off (or silent) at all times. The Bluetooth functionality of a mobile phone should be switched off during school time and may not be used to send images or files to other mobile phones. Mobile phones and personal devices are not permitted to be used in certain areas within the academy site such as classrooms and toilets. Staff are advised that in an emergency designated areas not used by pupils could be used i.e.. Staff Room, an SLT Office, car park, or in a member of staff's own car.

If staff feel there is a need to have their phone with them for a specific academy event i.e., Parents' evening the mobile phone should be switched to silent and should not be visible or intrude in the discussion with parents.

Unsuitable / Inappropriate Activities

Users shall not visit internet sites, make, post, download, upload, communicate or pass on materials, comments that contain	Child sexual abuse images
	Promote or conduct illegal acts e.g. under the child protection, obscenity, computer misuse and fraud legislation
	Adult material that potentially breaches the Obscene Publications Act in the UK
	Criminally racist materials in the UK
	Pornography
	Promotion of any type of discrimination
	Promotion of racial or religious hatred



or relate to:	Threatening behaviour, including the promotion of physical violence or mental harm
	Any other information which may be offensive to colleagues of the school or breaches the ethos of the academy or brings it into disrepute.

Incidents:	Refer to line manager	Refer to Exec Principal	Refer to LEA / MAT / HR	Refer to police	Refer to Conco for action	Warning given - Exec Principal	Suspension from school	Disciplinary action
Deliberately accessing or trying to access material that is considered to be illegal				✓				
Excessive or inappropriate personal use of the internet / social networking / instant messaging / email	✓				✓			
Unauthorised downloading / uploading of inappropriate files / information		✓			✓			
Allowing unauthorised staff / persons to access academy network by sharing the username and or password		✓			✓			
Careless use of personal data e.g., holding or transferring data in an insecure manner	✓	✓						
Deliberate actions to breach data protection or network security		✓						
Intentionally corrupting or destroying the data of other users of the network. Causing deliberate damage to hardware / software		✓						✓
Sending an email, text message or communication that is regarded as offensive or of a bullying or harassing nature	✓	✓						✓
Using personal email / social networking / instant messaging to communicate with student / pupils under the age of 18.		✓	✓	✓				
Actions that could compromise the professional standing of the staff member.	✓	✓						
Actions that could bring the academy into disrepute or breach the integrity of the academy.	✓	✓						
Accidentally accessing offensive or pornographic material and failing to report this to SLT.	✓	✓						



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

Staff Name:

.....

Signed:

.....

Date:

.....

Appendix 3



Acceptable Use Policy (AUP) for **PARENTS**



Background

We ask all children, young people and adults involved in the life of Brewwood to sign an Acceptable Use* Policy (AUP) to outline how we expect them to behave when they are online, and/or using academy networks, connections, internet connectivity and devices, cloud platforms and social media (both when on the academy site and outside of the academy).

Your child has also signed an AUP which has been sent home. We tell your children that **they should not behave any differently when they are out of school or using their own device or home network.**

What we tell pupils about behaviour and respect applies to all members of the academy community, whether they are at home or school:

“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.”

Where can I find out more?

You can read Brewwood's full Online Safety Policy <http://www.brewwood.staffs.sch.uk/wp-content/uploads/bsk-pdf-manager/2020/09/BMA-e-safety-Policy.pdf> for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding Policy, Behaviour Policy, etc). If you have any questions about this AUP or our approach to online safety, please speak to Mrs Priestley (Assistant Principal)

What am I agreeing to?

1. I understand that Brewwood CE Middle Academy uses technology as part of the daily life of the academy when it is appropriate to support teaching & learning and the smooth running of the academy, and to help prepare the children and young people in our care for their future lives.
2. I understand that the academy takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials, including behaviour policies and agreements, physical and technical monitoring, education and support and web filtering. However, the academy cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, which can sometimes be upsetting.
3. I understand that internet and device use in academy, and use of academy-owned devices, networks and cloud platforms out of school may be subject to filtering and monitoring. These should be used in the same manner as when in the academy, **including during any remote learning periods.**
4. I will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the academy staff, volunteers, LAC members, contractors, pupils or other parents/carers.

5. The impact of social media use is often felt strongly in schools, which is why we expect certain behaviours from pupils when using social media. I will support the academy's social media policy and not encourage my child to join any platform where they are below the minimum age.
6. I will follow the academy's digital images and video policy, which outlines when I can capture and/or share images/videos. I will not share images of other people's children on social media and understand that there may be cultural or legal reasons why this would be inappropriate or even dangerous. The academy sometimes uses images/video of my child for internal purposes such as recording attainment, but it will only do so publicly if I have given my consent on the relevant section of the Pupils Planner Page 3.
7. I understand that for my child to grow up safe online, s/he will need positive input from the academy and home, so I will talk to my child about online safety.
8. I understand that my child needs a safe and appropriate place to do remote learning if the academy or bubbles are closed (similar to regular online homework). When on any video calls with school, it would be better not to be in a bedroom but where this is unavoidable, my child will be fully dressed and not in bed, and the camera angle will point away from beds/bedding/personal information etc. Where it is possible to blur or change the background, I will help my child to do so.
9. If my child has online tuition for catchup after lockdown or in general, I will undertake necessary checks where I have arranged this privately to ensure they are registered/safe and reliable, and for any tuition remain in the room where possible, and ensure my child knows that tutors should not arrange new sessions or online chats directly with them.
10. I understand that whilst home networks are much less secure than school ones, I can apply child safety settings to my home internet. Internet Matters provides guides to help parents do this easily for all the main internet service providers in the UK. There are also child-safe search engines e.g. swiggle.org.uk and YouTube Kids is an alternative to YouTube with age appropriate content.
11. I understand that it can be hard to stop using technology sometimes, and I will talk about this to my children, and refer to the principles of the Digital 5 A Day: childrenscommissioner.gov.uk/our-work/digital/5-a-day/
12. I understand and support the commitments made by my child in the Acceptable Use Policy (AUP) which s/he has signed, and which can be seen here [Microsoft Word - AUP Pupils KS2.docx \(brewood.staffs.sch.uk\)](#) or [Microsoft Word - AUP Pupils KS3.docx \(brewood.staffs.sch.uk\)](#) and I understand that s/he will be subject to sanctions if s/he does not follow these rules.
13. I can find out more about online safety at Brewwood by reading the full Online Safety Policy here <http://www.brewood.staffs.sch.uk/wp-content/uploads/bsk-pdf-manager/2020/09/BMA-e-safety-Policy.pdf> and can talk to my child's class teacher or a member of SLT if I have any concerns about my child/ren's use of technology, or about that of others in the community, or if I have questions about online safety or technology use in the academy.

I/we have read, understood and agreed to this policy.

Signature/s:

Name/s of parent / guardian:

Parent / guardian of:

Date:



Appendix 4

Brewwood Middle CE Academy

Visitors / Volunteers Acceptable Use Policy Agreement Jan 2025

New technologies have become integral to the lives of children and young people in today's society, both within schools / academies 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 access to the internet and digital technologies 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 / academy 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 technology in their everyday work.

The academy will try to ensure that visitors and volunteers will have good access to digital technology to enhance their work, enable them to participate in meetings and to enhance learning opportunities for *students / pupils* learning and will, in return, expect visitors and volunteers to agree to be responsible users. Upon arrival at school, where a need to use IT is agreed by the Executive Principal, visitors and volunteers will be asked to sign this agreement.

Acceptable Use Policy Agreement - Visitors

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

For my professional and personal safety:

- I understand that the *school / academy* will monitor my use of the academy's digital technology and communications systems.
- 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 immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using *school / academy* 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.

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

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using *school / academy* equipment. I will also follow any additional rules set by the *school / academy* 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 use personal email addresses on the school / academy ICT systems.
- 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 that my data is regularly backed up.
- 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 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 / academy policies.
- I will not disable or cause any damage to school / academy 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 School / Academy / LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted / password protected. Paper based protected and restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student / 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 / academy policy to disclose such information to an appropriate authority.

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

- I understand that this Acceptable Use Policy applies not only to my work and use of school / academy digital technology equipment in school, but also applies to my use of school / academy 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 / academy

Communications

Actions in school time:	Allowed	Allowed at certain times	Not allowed
Mobile phones may be brought into school – but turned off in accordance with our safeguarding procedures?	✓		
Use of personal mobile phones in lesson time			✓
Taking photographs of pupils on mobile phones			✓
Accessing personal email addresses whilst in school using the academy network			✓
Use of chatrooms / social networking whilst in school			✓
Use of instant messaging whilst in lessons			✓
Use of personal blogs			✓

Unsuitable / inappropriate activities

Users shall not visit internet sites, make, post, download, upload, communicate or pass on materials, comments that contain or relate to:	Child sexual abuse images
	Promote or conduct illegal acts e.g. under the child protection, obscenity, computer misuse and fraud legislation
	Adult material that potentially breaches the Obscene Publications Act in the UK
	Criminally racist materials in the UK
	Pornography
	Promotion of any type of discrimination
	Promotion of racial or religious hatred
	Threatening behaviour, including the promotion of physical violence or mental harm
	Any other information which may be offensive to colleagues of the academy or breaches the ethos of the academy or brings it into disrepute.

Visitors / Volunteers Acceptable Use Policy Agreement Jan 2025

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

Visitor / Volunteer Name:

Signed:

Date:



Appendix 5

Brewwood Middle CE Academy

Supply Staff Acceptable Use Policy Agreement – Jan 2025

New technologies have become integral to the lives of children and young people in today's society, both within schools / academies 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 access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- that supply staff will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school / academy 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 technology in their everyday work.

The academy will try to ensure that supply staff will have good access to digital technology to enhance learning opportunities for *students / pupils* learning and will, in return, expect supply staff to agree to be responsible users. Upon arrival at the academy, where a need to use IT is agreed by the Executive Principal, supply staff will be asked to sign this agreement.

Staff and pupils will be asked to agree to follow the acceptable use policies each time they log on to the computer.

Acceptable Use Policy Agreement

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

For my professional and personal safety:

- I understand that the *school / academy* will monitor my use of the academy digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the academy digital technology 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 immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using *school / academy* 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 academy'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 academy website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only communicate with students / pupils and parents / carers using official academy systems. Any such communication will be professional in tone and manner. I will not engage in any on-line activity that may compromise my professional responsibilities.

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

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using *school / academy* equipment. I will also follow any additional rules set by the *school / academy* 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 use personal email addresses on the *school / academy* ICT systems.
- 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 that my data is regularly backed up.
- 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 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 / academy* policies.
- I will not disable or cause any damage to *school / academy* 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 *School / Academy / LA Personal Data Policy* (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted / password protected. Paper based Protected and restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student / 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 / academy* 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.

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

- I understand that this Acceptable Use Policy applies not only to my work and use of *school / academy* digital technology equipment in school, but also applies to my use of *school / academy* 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 / academy*

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Local Academy Board and / or the Local Authority and in the event of illegal activities the involvement of the police.

Communications

Actions in school time:	Allowed	Allowed at certain times	Not allowed
Mobile phones may be brought into the academy – (but turned off in accordance with our safeguarding procedures.)	✓		
Use of personal mobile phones in lesson time			✓
Use of personal mobile phones in social time (in accordance with the academy's staff behaviour policy)	✓		
Taking photographs of pupils on mobile phones			✓
Taking photographs on other academy camera devices	✓		
Use of hand held devices e.g. PDA's, school i-pads, tablets in lesson time		✓	
Accessing personal email addresses whilst in school using the academy network			✓
Use of academy email address for personal e-mails / communication		✓	
Use of chatrooms / social networking whilst in school			✓
Use of instant messaging whilst in lessons			✓
Use of instant messaging whilst in school (in accordance with the academy's staff behaviour policy)		✓	
Use of personal blogs			✓

Unsuitable / inappropriate activities

Users shall not visit internet sites, make, post, download, upload, communicate or pass on materials, comments that contain or relate to:	Child sexual abuse images
	Promote or conduct illegal acts e.g. under the child protection, obscenity, computer misuse and fraud legislation
	Adult material that potentially breaches the Obscene Publications Act in the UK
	Criminally racist materials in the UK
	Pornography
	Promotion of any type of discrimination
	Promotion of racial or religious hatred
	Threatening behaviour, including the promotion of physical violence or mental harm
	Any other information which may be offensive to colleagues of the school or breaches the ethos of the academy or brings it into disrepute.

Incidents:	Refer to Head of Key Stage/	Removal of network / internet access rights	Refer to Exec Principal	Refer to technical support staff for action re filtering /	Refer to the police
Deliberately accessing or trying to access material that could be considered illegal –	x	x	x		x
Unauthorised use of non-educational sites during lessons	x	x	x		
Unauthorised use of mobile phone / digital camera / other handheld device – asked to turn off on arrival	x	x	x		x
Unauthorised use of social networking / instant messaging / personal email	x	x	x		
Unauthorised downloading or uploading of files	x	x	x		
Allowing others to access academy network by sharing username and passwords – visitors / volunteers wouldn't access network, would they?	x	x	x		
Attempting to access or accessing the academy's network, using the account of a member of staff	x	x	x		
Corrupting or destroying the data of other users	x	x	x		
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	x	x	x		



Continued infringements of the above, following previous warnings or sanctions	x	x	x		
Actions which could bring the academy into disrepute or breach the integrity of the ethos of the academy	x	x	x		
Using proxy sites or other means to subvert the academy's filtering system	x	x	x		
Accidentally accessing offensive or pornographic material and failing to report the incident	x	x	x		x
Deliberately accessing or trying to access offensive or pornographic material	x	x	x		x
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	x	x	x		

Supply Staff Acceptable Use Policy Agreement Jan 2025

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

Visitor / Volunteer Name:

Signed:

Date:

Appendix 6

Access to Electronic Mail and the Internet



ACCESS TO ELECTRONIC MAIL AND THE INTERNET

We are pleased to offer all pupils at Brewwood CE (C) Middle Academy access to electronic mail and the Internet. In order to do this, pupils must have permission from a person with parental responsibility and must sign this form.

Access to email and the internet will enable pupils to explore thousands of libraries, databases and bulletin boards while exchanging messages with internet users throughout the world. However, parents and guardians should be warned that although we use a 'filtered' service provided by Concero (this means that offensive material is vetted and locked out of our system), some material may contain items that are illegal, defamatory, inaccurate and potentially offensive to some people. While our intent is to make internet access available to further educational goals and objectives, students may find ways to access other materials as well. We believe that the benefits to pupils, from access to the internet, exceed any disadvantages. Ultimately, parents and guardians of pupils are responsible for setting and conveying the standards that children should follow when using media and information sources, therefore Brewwood CE Middle Academy support and respect each family's right to decide whether or not to apply for access.

As much as possible, pupils will be directed to information resources that have been reviewed and evaluated prior to use. While pupils may be able to move beyond those resources to others that have not been evaluated by staff, they shall be provided with guidelines and lists of resources suitable for their research. Children will be supervised by a member of staff when using the email or internet facilities.

The following are not permitted:

- Sending or displaying offensive messages or pictures
- Accessing undesirable material
- Violating copyright laws
- Trespassing in another's work or file
- Intentionally wasting limited resources
- Using the network for commercial purposes

Violations will result in a loss of access as well as other disciplinary action.

The academy reserves the right to have full access to all pupil emails.

As a user of the academy's internet and email facilities, I hereby agree to comply with the above stated rules:

Pupil Signature..... Date.....

As the person with parental responsibility of the pupil signing above, I grant permission for my child to access the internet and email facility at Brewwood CE Middle Academy. I understand that some materials on the internet may be objectionable, but I accept responsibility for my child to follow the above stated rules when selecting, sharing and exploring information and media.

Signed..... Signature of person with parental responsibility

Date



Appendix 7

Mobile Phone Policy



Introduction and Aims

At Brewood CE Middle Academy the welfare and well-being of our pupils is paramount. The aim of the Mobile Phone Policy is to allow users to benefit from modern communication technologies, whilst promoting safe and appropriate practice through establishing clear and robust acceptable mobile user guidelines. This is achieved through balancing protection against potential misuse with the recognition that mobile phones are effective communication tools.

Scope

This policy applies to all individuals who have access to personal mobile phones on site. This includes staff, volunteers, committee members, children, young people, parents, carers, visitors and contractors. This list is not exhaustive.

This policy should also be read in relation to the following documentation:

- ☐ Safeguarding Children Policy
- ☐ Anti-Bullying Policy
- ☐ Guidance on the Use of Photographic Images and Videos of Children in Schools

Code of conduct

A code of conduct is promoted with the aim of creating a cooperative workforce, where staff work as a team, have high values and respect each other; thus creating a strong morale and sense of commitment leading to increased productivity.

Our aim is therefore that all practitioners:

- have a clear understanding of what constitutes misuse.
- know how to minimise risk.
- avoid putting themselves into compromising situations which could be misinterpreted and lead to possible allegations.
- understand the need for professional boundaries and clear guidance regarding acceptable use.
- are responsible for self-moderation of their own behaviours.
- are aware of the importance of reporting concerns promptly.

It is fully recognised that imposing rigid regulations on the actions of others can be counterproductive. An agreement of trust is therefore promoted regarding the carrying and use of mobile phones within the setting, which is agreed to by all users:

Personal Mobiles - Staff

- ☐ Staff should have their phones on silent or switched off and out of sight (e.g. in a drawer, handbag or pocket) during class time.
- ☐ Mobile phones should not be used in a space where children are present (e.g. classroom, playground).
- ☐ Use of phones (including receiving/sending texts and emails) should be limited to non-contact time when no children are present e.g. in office areas, staff room, empty classrooms.
- ☐ It is also advised that staff security protect access to functions of their phone.
- ☐ Should there be exceptional circumstances (e.g. acutely sick relative), then staff should make the Principal aware of this and can have their phone in case of having to receive an emergency call.
- ☐ Staff are not at any time permitted to use recording equipment on their mobile phones, for example: to take recordings of children, or sharing images. Legitimate recordings and photographs should be captured using academy equipment such as cameras and ipads.
- ☐ Staff should report any usage of mobile devices that causes them concern to the Headteacher.

Personal Mobiles – Pupils

We recognise that mobile phones are part of everyday life for many children and that they can play an important role

in helping pupils to feel safe and secure. However, we also recognise that they can prove a distraction in school and can provide a means of bullying or intimidating others. Therefore:

- Mobile phones should be switched off at the start of the day and kept in pupil's bags for the duration of the day. This follows a signed agreement from parents that their child will abide by the rules of the academy re. mobile phone use.
- Pupils are not permitted to have mobile phones in lessons or on academy visits unless permission is given by the leader e.g., for a European visit.
- Mobile phones brought into lessons will be confiscated and kept securely in the academy office to await collection by an adult with parental responsibility. If a parent cannot collect the phone on the same day, it will be stored securely in the academy office until a parent collects it.
- No images are to be taken using a mobile phone camera.
- No images are to be posted on any internet or social network sites.
- No Kindles or tablets are to be brought into the academy.

Beyond the academy day we:

- Strongly advise not to use mobile phones inappropriately or in a way which may bring the reputation of the academy into disrepute, or which might cause distress to any members of the community.

Volunteers, Visitors, LAC members and Contractors

All Volunteers, Visitors, LAC members and Contractors are expected to follow our mobile phone policy as it relates to staff whilst on the premises.

On arrival, such visitors will be informed of our expectations around the use of mobile phones.

Parents

While we would prefer parents not to use their mobile phones while at academy, we recognise that this would be impossible to regulate and that many parents see their phones as essential means of communication at all times.

We therefore ask that parents' usage of mobile phones, whilst on the academy site is *courteous* and *appropriate* to the academy environment.

We also allow parents to photograph or video academy events such as shows or sports day using their mobile phones – **but insist that parents do not publish images (e.g., on social networking sites) that include any children other than their own.**

Dissemination

The mobile phone policy will be shared with staff and volunteers as part of their induction. It will also be available to parents via the academy office and website.

Appendix 8

Academy Technical Security Policy Template (including filtering and passwords)

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The academy will be responsible for ensuring that the academy 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 (other than that allowed for monitoring purposes within the academy's policies).
- access to personal data is securely controlled in line with the academy's personal data policy.
- logs are maintained of access by users and of their actions while users of the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of academy computer systems.
- there is oversight from senior leaders and these have impact on policy and practice.

Responsibilities

The management of technical security will be the responsibility of Network manager CONCERO

Technical Security

Policy statements

The academy will be responsible for ensuring that the academy 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 will receive guidance and training and will be effective in carrying out their responsibilities:

- Academy technical systems will be managed in ways that ensure that the academy meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of academy technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted
- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, workstations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the systems and data.
- Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff.
- All users will have clearly defined access rights to academy technical systems.
- Users will be made responsible 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.
- Tony Bailey is responsible for ensuring that software license logs are accurate and up to date and that regular checks are made to reconcile the number of licenses purchased against the number of software installations.
- Mobile device security and management procedures are in place.
- Academy technical staff regularly monitor and record the activity of users on the academy technical systems and users are made aware of this in the Acceptable Use Agreement.
- Remote management tools are used by staff to control workstations and view users activity

- Malicious programs should not be used on academy networks. Any intentional use will result in disciplinary action.
- Staff may use laptops and other devices at home for non-academy use in an appropriate manner that does not breach any academy requirements.
- Removable media (e.g., memory sticks / CDs / DVDs) may be used appropriately by users on academy devices. Any malicious activity will result in disciplinary action.
- The academy infrastructure and individual workstations are protected by up-to-date software to protect against malicious threats from viruses, worms, Trojans etc.
- Personal data cannot be sent over the internet or taken off the academy site unless safely encrypted or otherwise secured.

Password Security

A safe and secure username / password system is essential if the above is to be established and will apply to all academy technical systems, including networks, devices, email and Office 365.

Policy Statements

- All users will have clearly defined access rights to academy technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually, by the Network Manager and Head of Computing.
- All academy networks and systems will be protected by secure passwords that are regularly changed
- The "administrator" passwords for the academy systems, used by the technical staff must also be available to the Principal or other nominated senior leader and kept in a secure place e.g., school safe. Consideration should also be given to using two factor authentication for such accounts.
- Passwords for new users, and replacement passwords for existing users will be allocated by Tony Bailey
- All users (adults and young people) 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.
- Users will change their passwords at regular intervals – as described in the staff and pupil sections below
- The level of security required will vary for staff and pupil accounts and the sensitive nature of any data accessed through that account.

Staff passwords:

- All staff users will be provided with a username and password by CONCERO who will keep an up to date record of users and their usernames.
- The password should be chosen to limit unwanted access. Staffs are recommended to use combinations of cases, numbers and not be obvious to guess.
- The account should be "locked out" following six successive incorrect log-on attempts
- passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)
- Should be changed at least every 60 to 90 days
- Should not re-used for 6 months and be significantly different from previous p the last four passwords cannot be re-used passwords created by the same user.
- Should be different for different accounts, to ensure that other systems are not put at risk if one is compromised
- Should be different for systems used inside and outside of the academy.

Pupil passwords

- All users will be provided with a username and password by CONCERO who will keep an up to date record of users and their usernames.
- Users will be required to change their password at key milestones during their time at the academy.
- Form tutors will be aware of the Password Stem and so can prompt pupils if they forget their password.

- Pupils will be taught the importance of password security and how this impacts on their own security in later life e.g online banking, internet use, online shopping etc.
- The complexity (i.e. minimum standards) will be set with regards to the cognitive ability of the children.

Training / Awareness

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

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

Pupils / students will be made aware of the academy's password policy:

- In lessons
- Through the Acceptable Use Agreement

Filtering

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; because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for Online safety and acceptable use. It is important that the academy has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this academy.

Responsibilities

The responsibility for the management of the academy's filtering policy will be held by Tony Bailey. They will manage the academy 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 academy filtering service must:

- be logged in change control logs.
- be reported to a second responsible person the Head of Computing.

All users have a responsibility to report immediately to (insert title) any infringements of the academy'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.

Policy Statements

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the academy. Illegal content is filtered by broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the academy to breaches of the filtering policy, which are.

then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the academy network, filtering will be applied that is consistent with academy practice.

- Either - The academy maintains and supports the managed filtering service (Safety Net Plus) provided by Entrust.
- The academy has provided enhanced / differentiated user-level filtering through the use of the Safety Net Plus filtering programme, allowing different filtering levels for different ages / stages and different groups of users.
- In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Principal.
- Mobile devices that access the academy internet connection (whether academy or personal devices) will be subject to the same filtering standards as other devices on the academy systems.
- Any filtering issues should be reported immediately to the filtering provider.
- Requests from staff for sites to be removed from the filtered list will be considered by the technical staff Tony Bailey (Network Manager). If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the online safety lead.

Education / Training / Awareness

Pupils 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:

- The Acceptable Use Agreement
- Induction training
- Staff meetings, briefings, Inset.

Changes to the Filtering System

Suitable requests for blocking and unblocking of sites will be made to Gavin Coulson. If reasonable requests they will be performed by Tony Bailey.

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 Gavin Coulson who will decide whether to make academy level changes (as above).

Monitoring

Brewood Middle Academy uses SENSO monitoring software to monitor staff and pupil use. Weekly logs are produced by James Dean and logged in a folder.

Other documents

Legislation

Academies should be aware of the legislative framework under which this E-Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;

- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The academy reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn

their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they: -

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the academy context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The academy is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

Links to other organisations or documents

The following links may help those who are developing or reviewing an academy e-safety policy.

Child Exploitation and Online Protection Centre (CEOP)

<http://www.ceop.gov.uk/>

ThinkUKnow

<http://www.thinkuknow.co.uk/>

CHILDNET

<http://www.childnet-int.org/>

INSAFE

<http://www.saferinternet.org/www/en/pub/insafe/index.htm>

BYRON REVIEW ("Safer Children in a Digital World")

<http://www.dcsf.gov.uk/byronreview/>

Becta

Website e-safety section - <http://schools.becta.org.uk/index.php?section=is>

Developing whole school policies to support effective practice:

<http://publications.becta.org.uk/display.cfm?resID=25934&page=1835>

Signposts to safety: Teaching e-safety at Key Stages 1 and 2 and at Key Stages 3 and 4:

<http://publications.becta.org.uk/display.cfm?resID=32422&page=1835>

"Safeguarding Children in a Digital World"

http://schools.becta.org.uk/index.php?section=is&catcode=ss_to_es_tl_rs_03&rid=13344

CYBER-BULLYING

DCSF - Cyberbullying guidance

<http://publications.teachernet.gov.uk/default.aspx?PageFunction=productdetails&PageMode=spectrum&ProductId=DCSF-00658-2007>

Teachernet

<http://www.teachernet.gov.uk/wholeschool/behaviour/tacklingbullying/cyberbullying/>

Teachernet "Safe to Learn – embedding anti-bullying work in schools"

<http://www.teachers.gov.uk/wholeschool/behaviour/tacklingbullying/safetolearn/>

Anti-Bullying Network - <http://www.antibullying.net/cyberbullying1.htm>

Cyberbullying.org - <http://www.cyberbullying.org/>

SOCIAL NETWORKING

Home Office Task Force - Social Networking Guidance -

<http://police.homeoffice.gov.uk/operational-policing/crime-disorder/child-protection-taskforce>

Digizen – "Young People and Social Networking Services":

<http://www.digizen.org.uk/socialnetworking/>

Ofcom Report:

http://www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/socialnetworking/summary/

Resources

SWGfL has produced a wide range of information leaflets and teaching resources, including films and video clips – for parents and school staff. A comprehensive list of these resources (and those available from other organisations) is available on the “SWGfL Safe” website:

http://www.swgfl.org.uk/safety/safetyresources.asp?page=schoolst_resources&audienceid=3

Links to other resource providers:

BBC Chatguides: <http://www.bbc.co.uk/chatguide/index.shtml>

Kidsmart: <http://www.kidsmart.org.uk/default.aspx>

Know It All - <http://www.childnet-int.org/kia/>

Cybersmart - <http://www.cybersmartcurriculum.org/home/>

NCH - <http://www.stoptextbully.com/>

Chatdanger - <http://www.chatdanger.com/>

Internet Watch Foundation: <http://www.iwf.org.uk/media/literature.htm>

Digizen – cyber-bullying films: <http://www.digizen.org/cyberbullying/film.aspx>

London Grid for Learning: <http://cms.lgfl.net/web/lgfl/safety/resources>

Glossary of terms

AUP	Acceptable Use Policy – see templates earlier in this document
Becta	British Educational Communications and Technology Agency (Government agency promoting the use of information and communications technology)
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD	Continuous Professional Development
CYPS	Children and Young Peoples Services (in Local Authorities)
DCSF	Department for Children, Schools and Families
ECM	Every Child Matters
FOSI	Family Online Safety Institute
HSTF	Home Secretary's Task Force on Child Protection on the Internet
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICTMark	Quality standard for schools provided by Becta
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
JANET	Provides the broadband backbone structure for Higher Education and for the National Education Network and RBCs.
KS1 ..	Key Stage 1 (2, 3, 4 or 5) – schools are structured within these multiple age groups eg KS3 = years 7 to 9 (age 11 to 14)



LA	Local Authority
LAN	Local Area Network
Learning Platform	A learning platform brings together hardware, software and supporting services to support teaching, learning, management and administration.
LSCB	Local Safeguarding Children Board
MIS	Management Information System
MLE	Managed Learning Environment
NEN	National Education Network – works with the Regional Broadband Consortia (eg SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
Ofsted	Office for Standards in Education, Children's Services and Skills
PDA	Personal Digital Assistant (handheld device)
PHSE	Personal, Health and Social Education
RBC	Regional Broadband Consortia (eg SWGfL) have been established to procure broadband connectivity for schools in England. There are 10 RBCs covering 139 of the 150 local authorities:
SEF	Self Evaluation Form – used by schools for self-evaluation and reviewed by Ofsted prior to visiting schools for an inspection
SRF	Self Review Form – a tool used by schools to evaluate the quality of their ICT provision and judge their readiness for submission for the ICTMark
SWGfL	South West Grid for Learning – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational e-safety programmes for schools, young people and parents.
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol



BREWOOD AND WHEATON ASTON FEDERATION

POLICY STATEMENT

Supporting pupils with medical needs and physical disabilities

We value and cherish every member of our community and celebrate their uniqueness.

Our values led curriculum promotes a love of life and learning inspiring every individual to be a respectful, resilient, and faithful global citizen.

"Let all that you do be done in love."

1 Corinthians 16:14

Respect, Faith, Resilience

We love and value each member of the St. Mary's family as precious individuals. Our outward-looking curriculum enables everyone to embrace life in all its fullness while celebrating the everyday and the unique. Through our Christian values of belief, respect and friendship we:

'Shine as a Light in the World'.

Matthew 5:16

Belief, Respect, Friendshi

Contents

1. Aims	2
2. Legislation and statutory responsibilities	2
3. Roles and responsibilities	3
4. Equal opportunities	4
5. Being notified that a child has a medical condition	4-4
6. Individual healthcare plans	4
7. Managing medicines	5-7
8. Emergency procedures	7
9. Training	7-8
10. Record keeping	7
11. Liability and indemnity	8
12. Complaints	8
13. Monitoring arrangements	8
14. Links to other policies	8
15. Appendix	9

1. Aims

This policy aims to ensure that:

- Pupils, staff and parents understand how our school will support pupils with medical conditions
- Pupils with medical conditions are properly supported to allow them to access the same education as other pupils, including school trips and sporting activities

The governing board will implement this policy by:

- Making sure sufficient staff are suitably trained.
- Making staff aware of pupils' conditions, where appropriate
- Making sure there are cover arrangements to ensure someone is always available to support pupils with medical conditions
- Providing supply teachers with appropriate information about the policy and relevant pupils
- Developing and monitoring individual healthcare plans (IHPs)

The named person with responsibility for implementing this policy is Lauren Guy, Inclusion Lead.

2. Legislation and statutory responsibilities

This policy meets the requirements under [Section 100 of the Children and Families Act 2014](#), which places a statutory duty on governing boards to effectively manage and meet the needs of pupils with medical conditions, medical needs and physical disabilities. The aim is to ensure that all children with medical conditions, in terms of both physical and mental health are properly supported by school.

It is also based on the Department for Education's statutory guidance on [supporting pupils with medical conditions at school](#).

3. Roles and responsibilities

3.1 The Local Academy Committee

The LAC has ultimate responsibility to make arrangements to support pupils with medical conditions. The governing board will ensure that sufficient staff have received suitable training and are competent before they are responsible for supporting children with medical conditions.

3.2 The Executive Principal

The Executive Principal will:

- Make sure all staff are aware of this policy and understand their role in its implementation
- Ensure that there is a sufficient number of trained staff available to implement this policy and deliver against all individual healthcare plans (IHPs), including in contingency and emergency situations
- Ensure that all staff who need to know are aware of a child's condition
- Take overall responsibility for the development of IHPs

- Make sure that school staff are appropriately insured and aware that they are insured to support pupils in this way
- Contact the school nursing service in the case of any pupil who has a medical condition that may require support at school, but who has not yet been brought to the attention of the school nurse
- Ensure that systems are in place for obtaining information about a child's medical needs and that this information is kept up to date

3.3 Staff

Supporting pupils with both physical and mental health medical conditions during school hours is not the sole responsibility of one person. Any member of staff may be asked to provide support to pupils with medical conditions, although they will not be required to do so. This includes the administration of medicines.

Those staff who take on the responsibility to support pupils with both physical and mental health medical conditions will receive sufficient and suitable training, and will achieve the necessary level of competency before doing so.

Teachers will take into account the needs of pupils with both physical and mental health medical conditions that they teach. All staff will know what to do and respond accordingly when they become aware that a pupil with a medical condition needs help.

3.4 Parents

Parents will:

- Provide the school with sufficient and up-to-date information about their child's medical needs
- Be involved in the development and review of their child's IHP and may be involved in its drafting
- Carry out any action they have agreed to as part of the implementation of the IHP, e.g. provide medicines and equipment, and ensure they or another nominated adult are contactable at all times
- Ensure that they sign the healthcare plan to confirm that they agree with the steps to be taken to support their child

3.5 Pupils

Pupils with both physical and mental health medical conditions will often be best placed to provide information about how their condition affects them. Pupils should be fully involved in discussions about their medical support needs and contribute as much as possible to the development of their IHPs. They are also expected to comply with their IHPs.

3.6 School nurses and other healthcare professionals

Our school nursing service will notify the school when a pupil has been identified as having a medical condition that will require support in school. This will be before the pupil starts school, wherever possible. They may also support staff to implement a child's IHP.

Healthcare professionals, such as GPs and [pediatricians](#), will liaise with the school's nurses and notify them of any pupils identified as having a medical condition. They may also provide advice on developing IHPs.

4. Equal opportunities

Our school is clear about the need to actively support pupils with both physical and mental health medical conditions to participate in school trips and visits, or in sporting activities, and not prevent them from doing so.

The school will consider what reasonable adjustments need to be made to enable these pupils to participate fully and safely on school trips, visits and sporting activities.

Risk assessments will be carried out so that planning arrangements take account of any steps needed to ensure that pupils with medical conditions are included. In doing so, pupils, their parents and any relevant healthcare professionals will be consulted.

5. Being notified that a child has a medical condition

When the school is notified that a pupil has a medical condition, the process outlined below will be followed to decide whether the pupil requires an IHP.

The school will make every effort to ensure that arrangements are put into place within 2 weeks, or by the beginning of the relevant term for pupils who are new to our school. See Appendix 1.

6. Individual healthcare plans

The Inclusion Lead has overall responsibility for the development of IHPs (Care Plans) for pupils with medical conditions along with ensuring that this plan has been reviewed and signed by parents of the child.. This has been delegated to Mrs Lauren Guy.

Plans will be reviewed at least annually, or earlier if there is evidence that the pupil's needs have changed.

Plans will be developed with the pupil's best interests in mind and will set out:

- What needs to be done
- When
- By whom

Not all pupils with a medical condition will require an IHP. It will be agreed with a healthcare professional and the parents when an IHP would be inappropriate or disproportionate. This will be based on evidence. If there is no consensus, the Executive Principal will make the final decision.

Plans will be drawn up in partnership with the school, parents and a relevant healthcare professional, such as the school nurse, specialist or pediatrician, who can best advise on the pupil's specific needs. The pupil will be involved wherever appropriate.

IHPs will be linked to, or become part of, any education, health and care (EHC) plan. If a pupil has SEN but does not have an EHC plan, the SEN will be mentioned in the IHP.

The level of detail in the plan will depend on the complexity of the child's condition and how much support is needed. The governing board and the Inclusion Lead will consider the following when deciding what information to record on IHPs:

- The medical condition, its triggers, signs, symptoms and treatments

- The pupil's resulting needs, including medication (dose, side effects and storage) and other treatments, time, facilities, equipment, testing, access to food and drink where this is used to manage their condition, dietary requirements and environmental issues, e.g. crowded corridors, travel time between lessons
- Specific support for the pupil's educational, social and emotional needs. For example, how absences will be managed, requirements for extra time to complete exams, use of rest periods or additional support in catching up with lessons, counselling sessions
- The level of support needed, including in emergencies. If a pupil is self-managing their medication, this will be clearly stated with appropriate arrangements for monitoring
- Who will provide this support, their training needs, expectations of their role and confirmation of proficiency to provide support for the pupil's medical condition from a healthcare professional, and cover arrangements for when they are unavailable
- Who in the school needs to be aware of the pupil's condition and the support required
- Arrangements for written permission from parents for medication to be administered by a member of staff, or self-administered by the pupil during school hours
- Separate arrangements or procedures required for school trips or other school activities outside of the normal school timetable that will ensure the pupil can participate, e.g. risk assessments
- Where confidentiality issues are raised by the parent/pupil, the designated individuals to be entrusted with information about the pupil's condition
- What to do in an emergency, including who to contact, and contingency arrangements

7. Managing medicines

Prescription medicines will be administered at school & on school visits:

- When it would be detrimental to the pupil's health or school attendance not to do so **and**
- Where we have parents' written consent

The only exception to this is where the medicine has been prescribed to the pupil without the knowledge of the parents.

Pupils under 16 will not be given medicine containing aspirin unless prescribed by a doctor.

Anyone giving a pupil any medication (for example, for pain relief) will first check maximum dosages and when the previous dosage was taken. Parents will always be informed.

The school will only accept prescribed medicines that are:

- In-date
- Labelled
- Provided in the original container, as dispensed by the pharmacist, and include instructions for administration, dosage and storage

The school will accept insulin that is inside an insulin pen or pump rather than its original container, but it must be in date.

All medicines will be stored safely. Pupils will be informed about where their medicines are at all times and be able to access them immediately, via a member of the admin team. Medicines and devices such as asthma inhalers, blood glucose testing meters, heart rate meters and adrenaline pens will always be readily available to pupils and not locked away. Mrs Guy will ensure that there are signed documentation to confirm that medication can be administered by academy staff.

Medicines will be returned to parents to arrange for safe disposal when no longer required.

7.1 Controlled drugs

Controlled drugs are prescription medicines that are controlled under the Misuse of Drugs Regulations 2001 and subsequent amendments, such as morphine or methadone.

A pupil who has been prescribed a controlled drug may have it in their possession if they are competent to do so, but they must not pass it to another pupil to use. All other controlled drugs are kept in a secure cupboard in the school office and only named staff have access.

Controlled drugs where a pupil has been prescribed such a drug will be easily accessible in an emergency and a record of any doses used and the amount held will be kept.

A controlled drug must be handed to a member of the admin team, the relevant form completed and it will then be stored in the locked office medicines cupboard, only the admin team/first aiders have access. If a pupil is on a school visit a named member of staff will keep the drug for the duration of the visit.

7.2 Pupils managing their own needs

Pupils who are competent will be encouraged to take responsibility for managing their own medicines and procedures. This will be discussed with parents and it will be reflected in their IHPs.

Pupils will be allowed to carry their own medicines and relevant devices wherever possible. Staff will not force a pupil to take a medicine or carry out a necessary procedure if they refuse, but will follow the procedure agreed in the IHP and inform parents so that an alternative option can be considered, if necessary.

7.3 Unacceptable practice

School staff should use their discretion and judge each case individually with reference to the pupil's IHP, but it is generally not acceptable to:

- Prevent pupils from easily accessing their inhalers and medication, and administering their medication when and where necessary
- Assume that every pupil with the same condition requires the same treatment
- Ignore the views of the pupil or their parents
- Ignore medical evidence or opinion (although this may be challenged)
- Send children with medical conditions home frequently for reasons associated with their medical condition or prevent them from staying for normal school activities, including lunch, unless this is specified in their IHPs
- If the pupil becomes ill, send them to the school office or medical room unaccompanied or with someone unsuitable

- Penalise pupils for their attendance record if their absences are related to their medical condition, e.g. hospital appointments
- Prevent pupils from drinking, eating or taking toilet or other breaks whenever they need to in order to manage their medical condition effectively
- Require parents, or otherwise make them feel obliged, to attend school to administer medication or provide medical support to their pupil, including with toileting issues. No parent should have to give up working because the school is failing to support their child's medical needs
- Prevent pupils from participating, or create unnecessary barriers to pupils participating in any aspect of school life, including school trips, e.g. by requiring parents to accompany their child
- Administer, or ask pupils to administer, medicine in school toilets

8. Emergency procedures

Staff will follow the school's normal emergency procedures (for example, calling 999). All pupils' IHPs will clearly set out what constitutes an emergency and will explain what to do.

If a pupil needs to be taken to hospital, staff will stay with the pupil until the parent arrives, or accompany the pupil to hospital by ambulance.

9. Training

Staff who are responsible for supporting pupils with medical needs will receive suitable and sufficient training to do so.

The training will be identified during the development or review of IHPs. Staff who provide support to pupils with medical conditions will be included in meetings where this is discussed.

The relevant healthcare professionals will lead on identifying the type and level of training required and will agree this with Inclusion Lead. Training will be kept up to date and appropriate records kept by the Inclusion Lead.

Training will:

- Be sufficient to ensure that staff are competent and have confidence in their ability to support the pupils
- Fulfil the requirements in the IHPs
- Help staff to have an understanding of the specific medical conditions they are being asked to deal with, their implications and preventative measures

Healthcare professionals will provide confirmation of the proficiency of staff in a medical procedure, or in providing medication.

All staff will receive training so that they are aware of this policy and understand their role in implementing it, for example, with preventative and emergency measures so they can recognise and act quickly when a problem occurs. This will be provided for new staff during their induction.

10. Record keeping

The governing board will ensure that written records are kept of all medicine administered to pupils for as long as these pupils are at the school. Parents will be informed if their pupil has been unwell at school.

IHPs are kept in a readily accessible place which all staff are aware of.

11. Liability and indemnity

The Local Academy Committee will ensure that the appropriate level of insurance is in place and appropriately reflects the school's level of risk.

12. Complaints

Parents with a complaint about their child's medical condition should discuss these directly with the Inclusion Lead or Executive Principal in the first instance. If they cannot resolve the matter, they will direct parents to the school's complaints procedure.

13. Monitoring arrangements

This policy will be reviewed and approved by the LAC annually

14. Links to other policies

This policy links to the following policies:

- Accessibility plan
- Complaints
- Equality information and objectives
- First aid
- Health and safety
- Safeguarding
- Special educational needs information report and policy
- Intimate Care Policy

Signed: Chair of Local Academy Committee Date:

Appendix 1: Being notified a child has a medical condition

