Holbrook Academy

Digital Technology Policy

Date Approved	
Signed	
Minuted	

Draft for approval

This policy takes account of the Academy's public sector equality duty set out in section 149 of the Equality Act 2010. It can be made available in large print or other accessible format if required. It applies wherever staff or volunteers are working with students even where this is away from the Academy, for example at an activity centre or on an educational visit.

Member of staff with responsibility for this policy.	K Newstead
Governor with responsibility for this policy.	Q&M Committee
Policy review date.	Spring term 2024
What is the purpose of this policy?	• Ensure the protection of confidentiality, integrity and availability of school information/assets. • Ensure all users are aware of and fully comply with key legislation. • Ensure all staff understand the need for information and ICT security and their own responsibilities in this respect.
What are its headline targets? (using quantitative and qualitative measures)	• No more than 5 instances of AUP guidance being broken by staff, students and/or parents/carers. • No more than 5 instances of peer-on-peer / e-safety related issues.
How is this policy to be judged as successful?	• Staff, students and parents/carers fully aware of, and comply with, key legislation resulting in fewer instances of breaking AUP agreement.

Contents

1. Introduction

Digital Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of digital technology within our society as a whole.

At Holbrook Academy, we understand the responsibility to educate our students on e-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom. This policy encompasses all aspects of e-Safety.

This policy and the Acceptable Use Agreements (included in the appendicies for staff, governors, visitors and students) are inclusive of both fixed and mobile internet; technologies provided by the Academy (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by students and staff, but brought onto Academy premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

2. Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students 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 e-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 e-safety behaviour that take place out of school.

3. Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the Academy.

3.1 Governors

Governors are responsible for the approval of the Digital Technology Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors Q&M Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of e-safety Governor (the role may be combined with that of the Safeguarding Governor). The role of the e-safety

Governor will include:

- regular meetings with the e-safety Co-ordinator
- regular monitoring of e-safety incident logs
- reporting to relevant Governors committee

3.2 Headteacher and Senior Leaders

The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the e-safety Co-ordinator.

The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (See flow chart on page 10 for dealing with e-safety incidents . Responding to incidents of misuse.)

- The Headteacher is responsible for ensuring that the e-safety Co-ordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher ensures that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the e-safety Co-ordinator.

3.3 e-safety Co-ordinator

The e-safety Co-ordinator is Mr Mark Taylor. In his absence, the Designated Safeguarding Lead will deal with any e-safety issues. The e-safety Co-ordinator will:

- lead the e-safety committee
- take day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the Academy e-safety policy
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Undertake regular and relevant training and meet statutory training requirements.
- Complete the T4T training and ensure that staff receive appropriate and regular training as part of statutory safeguarding training requirements.
- liaise with the Local Authority / relevant body
- liaise with Academy technical staff
- receive reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- monitor network / internet / incident logs and share these with relevant stakeholders.
- meet regularly with e-safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attend relevant committee of Governors
- report regularly to Senior Leadership Team

3.4 Network Manager

It is the responsibility of the Academy to ensure that the managed service provider carries out all the e-safety measures that would otherwise be the responsibility of the Academy technical staff, as suggested below. It is important that the managed service provider is fully aware of the Academy e-safety policy and procedures.

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 e-safety technical requirements and any Local Authority or other relevant body e-safety Policy or 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
- the filtering policy (if it has one), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person. (See appendix B : Technical Security Policy.)
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher and e-safety Co-ordinator for investigation / action / sanction.
- that monitoring systems are implemented and updated as agreed in Academy policies

3.5 Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current Academy e-safety policy and practices and attend relevant training.
- they have read, understood and signed the Staff Acceptable Use Agreement (AUA)
- they report any suspected misuse or problem to the Headteacher; E-safety Co-ordinator for investigation / action / sanction using Academy safeguarding reporting procedures.
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official Academy systems
- e-safety issues are embedded in all aspects of the curriculum and other activities

- students understand and follow the e-safety and acceptable use policies

- students 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

3.6 Safeguarding Designated Lead

Should be trained in e-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

It is important to emphasise that e-safety issues are safeguarding issues, not technical issues, simply that the technology provides additional means for safeguarding issues to develop.

The DSL and E-safety lead will discuss and agree actions and responses to breaches of e-safety expectations.

3.7 e-safety Group

The e-safety Group provides a consultative group that has wide representation from the Academy community, with responsibility for issues regarding e-safety and the monitoring the Digital Technology/Acceptable Use policy including the impact of initiatives. This role will be undertaken by the Pastoral Team. The group will also be responsible for regular reporting to the Governing Body.

Members of the e-safety Group (or other relevant group) will assist the e-safety Co-ordinator with:

- agreeing sanctions and follow up for breaches of the AUP
- the review and monitoring of the Academy e-safety policy
- the review of the Academy filtering policy and requests for filtering changes
- mapping and reviewing the e-safety curricular provision – ensuring relevance, breadth and progression

3.8 Students

- are responsible for using the Academy IT systems in accordance with the Student Acceptable Use Agreement

- are expected to 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 e-Safety practice when using digital technologies out of school and realise that the Academy's Digital Technology / Acceptable Use Agreement covers their actions out of school, if related to their membership of the Academy

- understand that they could lose access to technology, privileges or could face other sanctions as per the Rewards & Behaviour Policy.

3.9 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, newsletters, website and information about national and local e-safety campaigns. Parents and carers will be encouraged to support the Academy in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at Academy events
- access to parents' sections of the website and on-line student records
- their children's personal devices in the Academy (where this is allowed)

Parents must understand their role and responsibility in reporting e-safety issues to ensure that young people can be kept safe. Parents can discuss reporting with the e-Safety lead, DSL or alternates and must follow reporting steps to external agencies such as CEOPS / Police as advised.

4. Policy Statements

4.1 Education – Students

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

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

- A planned e-Safety curriculum should be provided as part of Computer Science, PHSEE/Life Skills and other lessons and should be regularly revisited

- Key e-Safety messages should be reinforced as part of a planned programme of assemblies and tutorial pastoral activities

- Students should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information.

- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

- Students must have access to examinations guidance and expectations around plagiarism and be guided in accordance with examinations rules. Students should be helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school

- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg 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.

4.2 Education – Parents / Carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's on-line behaviours. Parents/Carers 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:

- Newsletters, website
- Parents/Carers e-safety evenings
- Reference to the relevant websites / publications, e.g.
    - www.swgfl.org.uk
    - www.saferinternet.org.uk/
    - http://www.childnet.com/parents-and-carers
    - https://www.thinkuknow.co.uk/
    - https://www.ceop.police.uk/Safety-Centre/

4.3 Education & Training – Staff

It is essential that all staff receive e-Safety training and understand their responsibilities, as outlined in this policy. Training will be offered by the e-Safety Co-ordinator as follows:

- A planned programme of formal e-safety training will be made available to staff as part of their CPD. This will be regularly updated and reinforced. An audit of the e-Safety training needs of all staff will be carried out regularly

- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the Academy e-Safety policy and Acceptable Use Agreements.

- The e-Safety Co-ordinator (or other nominated person) will receive regular updates through attendance at external training events (eg from LA, other relevant organisations) and by reviewing guidance documents released by relevant organisations and ensure information is disseminated to stakeholders

4.4 Training – Governors

Governors should take part in e-safety awareness sessions, with particular importance for those who are members of any sub committee involved in technology, e-safety, health and safety and safeguarding. This may be offered in a number of ways:

- Governor e-safety training sessions
- Participation in Academy training:
    - information sessions for staff or parents
    - attendance at assemblies
    - e-Safety lessons

4.5 Technical infrastructure, filtering and monitoring

If the Academy has a managed IT service provided by an outside contractor, it is the responsibility of the Academy to ensure that the managed service provider carries out all the e-Safety measures that would otherwise be the responsibility of the Academy, as suggested below. It is also important that the managed service provider is fully aware of the Academy's Digital Technology Policy (encompassing e-Safety) and the Acceptable Use Agreements.

The Academy will be responsible for ensuring that the Academy infrastructure 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 e-Safety responsibilities.

A more detailed Technical Security Policy can be found in the appendix B.

- Academy technical systems will be managed in ways that ensure that the Academy meets recommended technical requirements as laid out by the Local Authority and other relevant organisations.

- 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

- 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 (Network

Manager) 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 term.

- The “administrator” passwords for the Academy IT system, used by the Network Manager must also be available to the Headteacher or other nominated senior leader and kept in a secure place.

- The Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations. Inadequate licencing could cause the Academy to breach the Copyright Act which could result in fines or unexpected licensing costs.

- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes (see appendix B for more details)

- The Academy has provided differentiated user-level filtering, allowing different filtering levels for different groups of users, e.g. staff, students.

- 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. The main monitoring software package is Impero.

- An appropriate system is in place for users to report any actual or potential technical incident or security breach.

- 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 systems and data. These are tested regularly. The Academy 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 systems.

- An agreed policy is in place regarding the extent of personal use that users, staff, students, others are allowed on Academy devices that may be used out of school.

- An agreed policy is in place that forbids staff from downloading executable files and installing programmes on Academy devices.

- An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on Academy devices. Personal data cannot be sent over the internet or taken off the Academy site unless safely encrypted or otherwise secured

5. Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students 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 students 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 made publicly available on social networking sites, nor should parents/carers comment on any activities involving other students in the digital/video images.

- Staff 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 students are appropriately dressed and are not participating in activities that might bring the individuals or the Academy into disrepute.

- Students must not take, use, share, publish or distribute images, video or sound recordings of others without their permission.

- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.

- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.

- Written permission from parents or carers will be obtained before photographs of students are published on the Academy website and is contained in the AUA signed by parents or carers at the start of the year. (see Parents / Carers Acceptable Use Agreement in the appendices)

6. Data Protection

In accordance with the Academy's Data Protection Policy, Information Management Handbook and the General Data Protection Regulation (GDPR), 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.

Following a number of 'high profile' losses of personal data by public organisations, schools are likely to be subject to greater scrutiny in their care and use of personal data.

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 has a Data Protection Policy

- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)

- Responsible persons are identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)

- Risk assessments are carried out

- It has clear and understood arrangements for the security, storage and transfer of personal data

- There are clear and understood policies and routines for the deletion and disposal of data

- 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 and 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. The Academy must provide approved software for encryption.

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 Academy policy (below) once it has been transferred or its use is complete

7. 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 disadvantages:

	Staff & other adults			Students / 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 school	✓				✓			
Use of mobile phones in lessons							✓	
Use of mobile phones in social time	✓							✓
Taking photos on mobile phones / cameras		✓					✓	
Use of other mobile devices eg tablets, gaming devices							✓	
Use of personal email addresses in school, or on school network								✓
Use of Academy email for personal emails								✓
Use of messaging apps								✓
Use of Google Meet	✓						✓	
Use of social media								✓
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. Staff and students should therefore use only the Academy email service to communicate with others when in school, or on Academy systems (e.g. by remote access).

- Users must immediately report, to the e-safety Co-ordinator, 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 students or parents/carers 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.

- Students will be provided with individual Academy email addresses for educational use

- Personal information should not be posted on the Academy website and only official email addresses should be used to identify members of staff

8. Social Media - Protecting Professional Identity

Expectations for teachers' professional conduct are set out in the current 'Teachers Standards'.

All schools, academies and local authorities have a duty of care to provide a safe learning environment for students and staff. The Academy 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 liable to the injured party.

The Academy provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the Academy 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 students, 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
- 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 e-safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

9. Unsuitable / Inappropriate Activities

Some internet activity eg accessing child abuse images or distributing racist material, is illegal and is obviously banned from the Academy and all other technical systems. Other activities eg cyber-bullying is banned and could lead to criminal prosecution.

There are, however, a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities. The Academy believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using Academy equipment or systems. he Academy policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	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 Academy or brings the Academy into disrepute				X	
Using Academy 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 (eg 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)		✓				
On-line gaming (non educational)			✓			
On-line gambling					✓	
On-line shopping / commerce				✓		
File sharing		✓				
Use of social media				✓		
Use of messaging apps				✓		
Use of video broadcasting eg Youtube				✓		

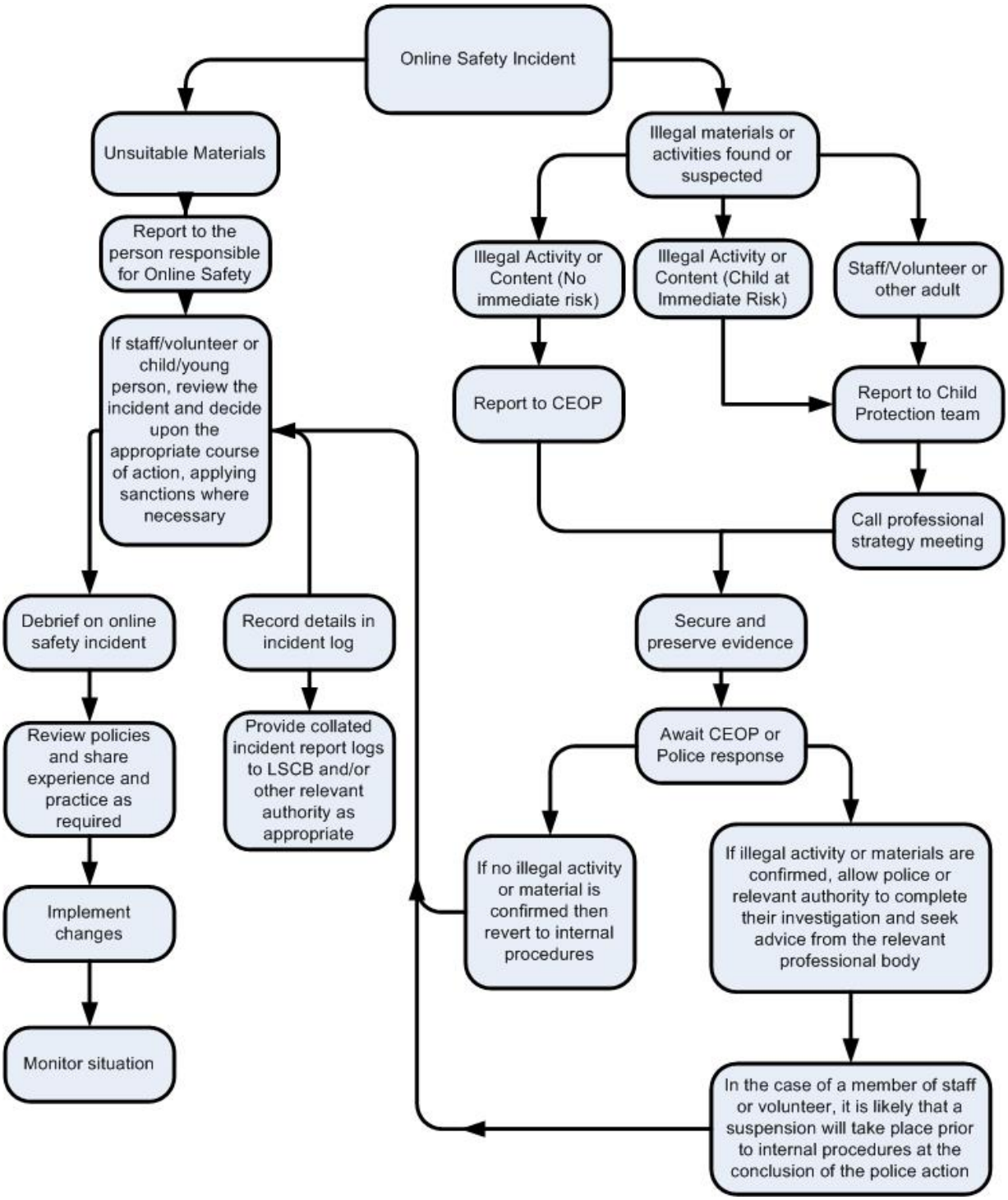
10. Responding to incidents of misuse

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.

10.1 Illegal Incidents

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

e-Safety Process



10.2 Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow the 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:

- Inform Headteacher and agree an action plan.

- 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.

10.3 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 school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour procedures as follows:

10.3.1 Staff

Incidents:	Actions / Sanctions							
	Refer to line managerr	**Refer to Headteacher**	**Refer to HR**	**Refer to Police**	**Refer to Technical Support Staff**	**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				
Inappropriate personal use of the internet / social media / personal email	X							
Unauthorised downloading or uploading of files	X				X	X		
Allowing others to access the Academy network by sharing username and passwords or attempting to access or accessing the Academy 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						
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
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X					X		
Actions which could compromise the staff member's professional standing	X							
Actions which could bring the Academy into disrepute or breach the integrity of the ethos of the		X	X			X		

Academy								
Using proxy sites or other means to subvert the Academy's filtering system		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
Breaching copyright or licensing regulations	X							
Continued infringements of the above, following previous warnings or sanctions		X	X					X

The Headteacher will update the LADO of any unacceptable staff behaviour which risks the safety and well being of children as per safeguarding expectations.

Appendices

Appendix A: Acceptable Use Agreements (AUA) for Students, Parents/Carers and Staff

Student Acceptable Use Agreement (AUA)

Academy Policy
Digital technologies have become integral to the lives of children and young people, both within schools and outside school. 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 Agreement 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 Academy 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 students will have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users.

Acceptable Use Agreement
I understand that I must use school IT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the IT 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 (unless I have permission) print out large (> 20 pages) documents. If I do so, I recognise that the Academy will recover the costs (paper and printing costs).
- I will not use the Academy systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), 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 and the Academy's 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 school if I have permission. I understand that mobile devices are not to be used during the Academy day (8:30am – 3.15pm) unless I have permission from a member of staff. 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 only use social media sites with permission and at the times that are allowed.

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 will comply with expectations set out by my teachers and examination boards around plagiarism, sourcing and referencing.

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

- 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 school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Agreement, I will be subject to disciplinary action. This may include loss of access to the Academy network / internet, detentions, fixed term exclusion, contact with parents and in the event of illegal activities, involvement of the police.

Student Sanction

Actions / Sanctions

The following sanction will be applied for any breach of this Agrteement.

Incidents:	Refer to Pastoral Team	Refer to eSafety Co-ordinator	Refer to Headteacher	Refer to Police	Refer to technical staff	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 Digital Policy).		X	X	X					X
Unauthorised use of non-educational sites during lessons		X			X	X	www		
Unauthorised use of mobile phone / digital camera / other mobile device						X			
Unauthorised use of social media / messaging apps / personal email		X			X	X	www		
Unauthorised downloading or uploading of files		X			X	X	NET		
Allowing others to access Academy network by sharing username and passwords		X			X			X	
Attempting to access or accessing the Academy network, using another student's account		X			X		NET	X	
Attempting to access or accessing the Academy network, using the account of a member of staff		X	X		X	X	NET		X
Corrupting or destroying the data of other users		X			X	X	NET		
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X				X	www		X
Continued infringements of the above, following previous warnings or sanctions			X			X	NET		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	www		
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X			X	X		X	
Deliberately accessing or trying to access		X	X	X	X	X			X

offensive or pornographic material									
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X							

www = Internet Access NET = Academy networks

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.

Student Acceptable Use Agreement Form

This form relates to the Student Acceptable Use Agreement, to which it is attached.

Please complete the sections below 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 IT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the Academy systems and devices (both in and out of school)
- I use my own devices in the Academy (when allowed) eg mobile phones, gaming devices, USB devices, cameras, etc
- I use my own equipment out of the Academy in a way that is related to me being a member of this Academy, eg. communicating with other members of the school, accessing Academy email, Go4Schools, website, etc

Name of Student	
Class	
Signed	
Date	

Parent/Carer Acceptable Use Agreement (AUA)

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They 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 communications technologies for educational, personal and recreational use.
- that Academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The Academy will try to ensure that students will have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users. A copy of the Student Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents/Carers are requested to sign the following statement in their child's Student Planner each year :-

> I have read the Academy's **Internet Acceptable Use Policy for Students**. I will instruct my child regarding any restrictions against accessing material that are in addition to the restrictions set out in the Policy. I will emphasise to my child the importance of following the rules for personal security and safety and will support the Academy in keeping all children safe online.
>
> Parent/Carer's Signature ……Date ……
>
> Parent/Carer's Name ...……...

Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Students and members of staff may use digital cameras to record evidence of activities in lessons and out of school. 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 Academy 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 school. We will also ensure that when images are published, the young people can not 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 in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students in the digital / video images.

Parents / carers are requested to sign the permission form shown below, when their child joins the Academy, to allow the Academy to take and use images of their children.

Dear Parent / Carer,

At Holbrook Academy, we sometimes take photographs of students. We use these photos on the Academy's website, in promotional materials, newsletters, in newspaper articles and on display boards around Academy.

We would like your consent to take photos of your child, and use them in the ways described above. If you are not happy for us to do this, that's no problem – we will accommodate your preferences.

Please tick the relevant box(es) below and return this form to school.

I am happy for the Academy to take photographs of my child. ☐

I am happy for photos of my child to be used on the Academy website. ☐

I am happy for photos of my child to be used in the promotional materials. ☐

I am happy for photos of my child to be used in internal displays. ☐

I am happy for photos of my child to be used in newsletters. ☐

I am happy for photos of my child to be in newspaper articles. ☐

I am NOT happy for the school to take or use photos of my child. ☐

If you change your mind at any time, you can let us know by emailing parents@holbrookacademy.org, calling the Academy on 01473 328317, or by visiting the main office.

If you have any other questions, please contact the main office.

Signature of Parent/Carer: …… Date: ……..

Name of Student: ……..

Use of Cloud Systems Permission Form

The Academy uses Google's G Suite, Go4Schools for students and staff. This permission form describes the tools and student responsibilities for using these services.

The following services are the main services available to each students and hosted by Google as part of the Academy's online presence in G Suite:

Mail - an individual email account for Academy use managed by the Academy

Calendar - an individual calendar providing the ability to organize schedules, daily activities, and assignments

Docs - a word processing, spreadsheet, drawing, and presentation toolset that is very similar to Microsoft Office

Drive – cloud storage facility

Classroom – online area for a specific class

Meet – Video/Audio conferencing, including Live Streaming (recorded for safety purposes) and pre-recorded video lessons.

Using these tools, students collaboratively create, edit and share files and websites for Academy related projects and communicate via email with other students and members of staff. These services are entirely online and available 24/7 from any Internet-connected computer. Examples of student use include showcasing class projects, building an electronic portfolio of Academy learning experiences, and working in small groups on presentations to share with others.

The Academy believes that use of the tools significantly adds to your child's educational experience.

Go4Schools gives the student access to subject's progress information (target grade, current grade, etc), behaviour points and reports.

As part of the Google terms and conditions we are required to seek your permission for your child to have a G Suite account and permission to access to other Cloud systems:

Parent / Carers Name	
Student Name	

As the parent / carer of the above students, I agree to my child using the Academy Google G Suite and other Cloud systems.	Yes / No
Signed	
Date	

Use of Biometric Systems for Cashless Catering

The Academy offers a fingerprint based biometric security system for children to obtain school meals. Parents/Carers are requested to complete the following details when their child joins the Academy:-

This system offers a number of benefits. These include removing the need for students to bring cash into school, avoiding the risk of it being lost or spent on other things. Parents/carers have the option of limiting their child's daily spend and enables them to 'top-up' students' accounts online.

The system requires students to place their fingertip on a scanner to make a payment for their food. This is their 'digital signature'. This 'signature' is stored and the system's software encrypts it into a set of letters and numbers which is hosted on our own school server.

We use a secure on-line payment system called ***'School Gateway'*** where your child's Cashless Catering account will be available to accept payments. The account can be topped up using a debit card, credit card or direct transfer and the balance, together with information about the items students have purchased, can be viewed at any time.

If you still require further information please email our Finance Manager.

Legislation requires permission to use this technology, so please would you complete this paperwork prior to your child starting at the Academy. We have included the option of a 'PIN' number rather than fingerprint although the fingerprint is our preference as 'PIN' numbers can be misused.

Please complete and return the permission slip to the Academy office.

……..……..

PERMISSION SLIP

Name of Student ……..… Year ……

☐ I give authorisation for Holbrook Academy to obtain biometric information from my daughter/son to be stored for no other use than for the Academy's administration systems. Such biometric information will be disposed of when the student leaves the school and images will be stored as data points and not as fingerprint images.

☐ Please supply a 'PIN' number for my daughter/son to use instead of using their fingertip on the scanner.

☐ My daughter/son will not be purchasing food from the canteen.

Signed: ……..…… Parent/Carer Date……

Staff (and Volunteer) Acceptable Use Agreement (AUA)

Academy Policy
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 internet access at all times.

This Acceptable Use Policy is intended to ensure:
- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that Academy IT 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 IT in their everyday work.

The Academy will try to ensure that staff and volunteers will have good access to IT to enhance their work, to enhance learning opportunities for students learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement
I understand that I must use Academy IT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the IT systems and other users. I recognise the value of the use of IT for enhancing learning and will ensure that students receive opportunities to gain from the use of IT. I will, where possible, educate the young people in my care in the safe use of IT and embed e-safety in my work with young people.

For my professional and personal safety:
- I understand that the Academy will monitor my use of the IT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of Academy IT systems (e.g .laptops, email, etc) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the Academy IT 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 Academy.
- 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 Academy IT 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 use chat and social networking sites in school in accordance with the Academy's policies.
- I will only communicate with studentss and parents / carers using official Academy systems. Any such communication will be professional in tone and manner. Staff should be made aware of the

risks attached to using their personal email addresses / mobile phones / social networking sites for such communications)
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The Academy has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the Academy:
- When I use my mobile devices (tablets / PDAs / laptops / 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 IT 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 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 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 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 Academy policies.
- I will not disable or cause any damage to 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 Information Management Handbook. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student 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 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.

When using the internet in my professional capacity or for Academy sanctioned personal use:
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the Academy:
- I understand that this Acceptable Use Policy applies not only to my work and use of Academy IT equipment in school, but also applies to my use of Academy IT 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. Please see the Academy's Behaviour Policy.

I have read and understand the above and agree to use the Academy IT 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 / Volunteer Name	
Signed	
Date	

Appendix B: Academy Technical Security Policy

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 the service provider, European Electronique (EE) as Network Manager.

Technical Security
Policy statements

The Academy will be responsible for ensuring that the Academy infrastructure / 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, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the Academy 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. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed annually by the E-Safety Committee
- 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.
- The Finance Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- 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
- A system is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the Academy system.
- An agreed policy is in place regarding the downloading of executable files and the installation of programmes on Academy devices by users

- An agreed policy is in place (to be described) regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on Academy devices
- 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 Virtual Learning Environments (VLE).

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 annually by the E-Safety Committee
- All Academy networks and systems will be protected by secure passwords
- The "master / administrator" passwords for the Academy systems, used by the technical staff must also be available to the Headteacherl or other nominated senior leader and kept in a secure place eg school safe.
- An Academy should never allow one user to have sole administrator access.
- 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.

Staff passwords:
- All staff users will be provided with a username and password by the Network Manager who will keep an up to date record of users and their usernames.
- temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on

Student passwords:
- All students will be provided with a username and password by the Network Manager who will keep an up to date record of users and their usernames.
- Students / pupils will be taught the importance of password security

Awareness:
Members of staff will be made aware of the Academy's password policy:
- at induction
- through the Academy's e-safety policy and password security policy
- through the Acceptable Use Agreement

Students will be made aware of the Academy's password policy:
- in lessons
- For KS3 this takes place at the beginning of each year during Computer Science lessons
- For KS4, this is covered during 'Form' time at the beginning of the year
- through the Acceptable Use Agreement

Protection from cyber attacks
Please see the glossary (Appendix C) to help you understand cyber security terminology.
The school will:
- Work with governors and the IT department to make sure cyber security is given the time and resources it needs to make the school secure

- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security, including how to:
    - Check the sender address in an email
    - Respond to a request for bank details, personal information or login details
    - Verify requests for payments or changes to information
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate whether our IT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Put controls in place that are:
    - **'Proportionate'**: the school will verify this using a third-party audit at least once a year to objectively test that what it has in place is up to scratch
    - **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe
    - **Up-to-date:** with a system in place to monitor when the school needs to update its software
    - **Regularly reviewed and tested**: to make sure the systems are as up to scratch and secure as they can be
- Back up critical data twice a day and store these backups in a way not connected to the network. Both local and offsite backups to be maintained for 15 days.
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to Suffolk County Council. Network security is provided by EE.
- Make sure staff:
    - Dial into our network using a virtual private network (VPN) when working from home
    - Enable multi-factor authentication where they can, on things like school email accounts
    - Store passwords securely using a password manager
- Make sure ICT staff conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights
- Have a firewall in place that is switched on
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and seeing if they have the Cyber Essentials certification
- Develop, review and test an incident response plan with the IT department, for example, including how the school will communicate with everyone if communications go down, who will be contacted when, and who will notify Action Fraud of the incident.

Monitoring

The responsible person Network Manager will ensure that full records are kept of:

- User Ids
- User log-ons
- Security incidents related to this policy

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 e-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 Network Manager. They will manage the Academy filtering, in line with this policy and will keep a log 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 e-safety Lead

All users have a responsibility to report immediately to the Network Manager 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.

- The Academy maintains and supports the managed filtering service provided by the Internet Service Provider
- 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 Network Manager. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Group.

Awareness
Students will be made aware of the importance of filtering systems through the e-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
- staff meetings, briefings, Inset.

Parents will be informed of the Academy's filtering policy through the Acceptable Use Agreement.

Changes to the Filtering System

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

Audit / Reporting

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

- the second responsible person (e-safety Lead)
- E-Safety Group

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

Further Guidance

Academies may wish to seek further guidance. The following is recommended:

NEN Technical guidance: http://www.nen.gov.uk/advice/266/nen-guidance-notes.html

Somerset Guidance for schools – this checklist is particularly useful where a school / Academy uses external providers for its technical support / security:
http://www.360safe.org.uk/Files/Documents/Questions-for-Technical-Support-Somerset.aspx

Appendix C: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber attack and the measures the school will put in place. They are from the National Cyber Security Centre (NCSC) glossary.

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (like bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.

TERM	DEFINITION
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programs designed to self-replicate and infect legitimate software programs or systems.
Virtual Private Network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly targeted phishing attacks (where emails are made to look legitimate) aimed at senior executives.

Addendum - ~~COVID-19~~ : Live Lessons

This outlines the procedures to be followed for online learning ie 'live lessons or live streaming' ~~during the COVID-19 lockdown~~.

1) Meeting must be scheduled on the 'Live Opportunities' calendar and a time posted to students on the Stream

2) 2 members of staff required for a live streaming Meet

3) Only use Google Meet and accessed via Google Classroom

4) Students unable to use Meet themselves

5) Only people with a *@holbrookacademy.org* account can join a Meet, unless agreed with e-safety lead and senior leaders and for specified Academy matters

6) Students can only join a meeting when a member of staff allow them to do so and a member of staff must remain in the 'Meet' until all students have left

7) All meeting must be recorded for safety purposes. Recordings will be retained for one term and then deleted at the end of the following term ie a meeting recorded on the last day of a term will be available until the end of the following term.

8) Staff must monitor the 'waiting' area and time before the formal commencement of the live learning session.

9) Once the recording starts, students must confirm their permission for recording again and be reminded of the following:

   This is a live learning opportunity. By being here, we are all agreeing to the Academy's acceptable use of ICT policies. Students can leave at any point. You may choose to contribute verbally or by using the chat facility. Students can choose to show video or not. A recording of this session will be retained as part of our safeguarding procedures. It will be deleted according to the timetable set out in point 7) above.

10) Once the recording starts get permission again so that it has been recorded. Suggest that a register is called and each student can then respond individually

11) School rules apply – See in school document *Google Meet and Working with Children*[1]

12) Attendance at a live learning opportunity is voluntary. Students should not feel pressurised to attend. Students with technology issues who would otherwise attend should discuss these with the Academy who will seek to resolve these.

Learning at home

During a period of 'Lockdown' ~~and phased re-opening for students~~, it is the expectation that staff and students will continue to work from home. The Academy will continue to develop technology solutions to support the delivery of the curriculum and students staying at home. Developments will be shared with families via Academy communication channels and, therefore, may not explicitly be mentioned in this policy.

E-safety will continue to factor in all decisions around technology during this time.

[1] https://docs.google.com/document/d/1lC7kslsu1oH2x_az5ebJfW32rV86zKWX1hNwfK-R4bQ/edit?usp=sharing