DOCUMENT CONTROL

Author/Contact	N Buglass Tel: 0117 379 0119 Email: info@educatetogether.org.uk	
Document Path & Filename	I Am Compliant/Policies and Procedures/Policy Stack 2019/Online Safety Policy_ETAT0015_20.1	
Document Reference	Online Safety Policy_ETAT0015	
Version	20.1	
Status	Approved	
Publication Date	May 2020	
Related Policies		
Review Date	May 2021	
Approved/Ratified by	CEO/ICT Group	Date: 11.5.2020

Distribution:

All staff through 'I Am Compliant' Policy file.

Please note that the version of this document contained within the Policy Folder on Staff General is the only version that is maintained.

Any printed copies should therefore be viewed as "uncontrolled" and as such, may not necessarily contain the latest updates and amendments.

Version	Date	Comments	Author
19.1	May 2016	ESafety Policy (ETAT0015)	Ros Farrell
20.1	March 2020	Replaces previous ESafety Policy, using same number	Emma Garnett/Sam O'Regan

Educate Together Academy Trust Online Safety Policy

Development / Monitoring / Review of this Policy

This Online Safety policy has been developed by ETAT IT Strategy group made up of:

- Headteacher / Senior Leaders
- Staff – including Teachers, Support Staff, Technical staff
- Governors / Board

Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the CEO and ICT Working Group:	11.5.2020
The implementation of this Online Safety policy will be monitored by the:	Safeguarding Lead on the Board, Interim COO and IT Consultant with support from Soltech IT and the ICT Working Group
Monitoring will take place at regular intervals:	Annually
The Board of Directors / Governing Body / Governors Sub Committee 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:	Annually
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:	May 2021

Should serious online safety incidents take place, the following external persons / agencies should be informed:	Board's Safeguarding Lead, CEO and Exec Head, LADO, Police and/or DPO

The school will monitor the impact of the policy using:

- Logs of reported incidents via Cpoms
- Monitoring logs of internet activity (including sites visited) / filtering
- Annual surveys / questionnaires of:
    - students / pupils
    - parents / carers
    - staff

Scope of the Policy

This policy applies to all members of the Educate Together Academy Trust community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of academy digital technology 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 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 online-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.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the Trust.

Role	**Responsibilities**
Trust Board	Trustees are responsible for the approval of the Online Safety Policy

Local Governing Bodies	The LGB is responsible for reviewing the effectiveness of the policy. The role of the LGB Online Safety Lead will include: • regular meetings with the Computing subject leader/Designated Safeguarding Lead • regular monitoring of online safety incident logs • regular monitoring of filtering / change control logs • reporting back to other committee members/Trust board
Headteacher and Senior Leaders	Ensure that all staff receive suitable CPD to carry out their Online Safety roles and sufficient resource is allocated. Ensure that there is a system in place for monitoring Online Safety - using CPOMS Follow correct procedure in the event of a serious Online Safety allegation being made against a member of staff. Inform the Trust Board about any serious Online Safety issues, including filtering. Ensure that the school infrastructure/network is safe and secure and that policies and procedures approved within this policy are implemented.
Designated Safeguarding Officer (in liaison with the Computing subject lead)	Deal with day to day Online Safety issues. Lead role in establishing/reviewing Online Safety policies and documents. Ensure all staff are aware of the procedures outlined in policies. Provide training and advice for staff. Attend SWGFL online safety live sessions. Liaise with technical staff. Deal with and log Online Safety incidents including changes to filtering. Meet with Local Governing Body Safeguarding Lead regularly to monitor Online Safety developments. Have up to date training 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

	• online-bullying
Head of IT	• Ensure that the academy's technical infrastructure is secure and is not open to misuse or malicious attack • Ensure that the academy meets required online safety technical requirements that this Online Safety Policy sets out and other relevant guidance that may apply. • Ensures that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed • Ensure 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 • Ensure that the use of the network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation. • Ensure that monitoring software / systems are implemented and updated as agreed in academy policies
Teaching and Support Staff	• Have an up to date awareness of online safety matters and of the current Academy Online Safety Policy and practices • Have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP) • Report any suspected misuse or problem to the Headteacher/DSL for investigation • Ensure that all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems • Online safety issues are embedded in all aspects of the curriculum and other activities • Ensure that pupils understand and follow the Online Safety Policy and acceptable use policies • Ensure that pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • Monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices • Ensure that 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.
Pupils	• Are responsible for using the Academy digital technology systems in accordance with the Pupil Acceptable Use Agreement which is shared at the beginning of each academic year with all children by the class teacher

	• 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 online-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, newsletters, letters, website and information about national / 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: 1. digital and video images taken at school events 2. access to parents' sections of the website and on-line student / pupil records 3. their children's personal devices in the academy (where this is allowed)
Community Users	Community Users who access Academy systems as part of the wider Academy provision will be expected to sign a Volunteer AUA before being provided with access to academy systems.

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 / digital literacy is therefore an essential part of the academy's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

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

- A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited – Academies will use the digital literacy programme to support this
- Key online safety messages should be reinforced as part of a planned programme of assemblies and classroom 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 supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- 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, pupils should be guided to sites checked as suitable for their use and 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, reporting any concerns via cpoms. Pupils will be taught to use Swiggle.org.uk for searches.
- 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 Head of IT (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:

- Curriculum activities
- Letters, newsletters, App and website
- Parents / Carers meetings/workshops
- High profile events such as Safer Internet Day
- Reference to the relevant web sites / publications e.g. 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 community groups / members of the community to gain from the academy's online safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and online safety
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The Academy website providing online safety information for the wider community

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 is 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 yearly.
- All new staff receive Online Safety training as part of their induction programme, provided by our Head of IT, ensuring that they fully understand the Academy Online Safety Policy and Acceptable Use Agreements.
- The DSL and Computing Lead will receive regular updates through attendance at external training events (eg from SWGfL / LA / other relevant organisations) 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/ INSET days.

- The DSL in liaison with the Computing Lead will provide advice / guidance / training to individuals as required.

Training – Trust Board/LGB

Trust Board members and members of the LGB will take part in online safety training / awareness sessions, with particular importance for those who are responsible for Online Safety and Safeguarding / health and safety. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / MAT / National Governors Association / or other relevant organisation (e.g. SWGfL).
- Participation in MAT training or information sessions for staff or parents.

Technical – infrastructure / equipment, filtering and monitoring

- 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
- All users will have clearly defined access rights to academy technical systems and devices.
- All users at Key Stage Two will be provided with a username and secure password by Head of IT/ Computing Lead who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- The “master / administrator” passwords for the school / academy ICT systems, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place.
- IT Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the 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

- There is a clear process in place to deal with requests for filtering changes (see appendix for more details)
- Internet filtering / monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet
- The academy has provided differentiated user-level filtering for pupils and staff.
- Users to report any actual / potential technical incident / security breach to the IT Manager and Head Teacher
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- Guests to the school who need temporary access to school systems will read and sign the Acceptable Use Policy for staff/visitors before any access is granted.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured such as One Drive or Global Scape.

Mobile Technologies

- The school Acceptable Use Agreements for staff, pupils/students and parents / carers will give consideration to the use of mobile technologies
- The school allows:

	School Devices		Personal Devices		
	School owned for single user	**School owned for multiple users**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	Yes	Yes	Yes, for UKS2 pupils *	Yes **	Yes***
Full network access	Yes	Yes	No	No	No

Internet only			No	Yes via Guest Network only if requested	Yes via Guest Network only if requested
No network access for any devices not belonging to school or the Academy Trust ***Pupil devices will be allowed with a prior signed written agreement between the parent and school. Devices will be switched off and stored in a locked cupboard throughout the school day. The school and its staff do not accept any liability for loss or damage of any devices sent into school.** **Devices may be purchased for pupils by third party providers. The use and storage of these devices must be under the discretion of the Headteacher and supporting IT team** **** Devices will be switched off and stored in a locked cupboard, with the exception of lunch times when they may be used in staff only areas.** ***** Regular Visitors will read and sign a copy of the acceptable use policy. Other visitors including contractors will be informed of the safeguarding requirements upon sign in. Devices will be switched off at all times unless used in a staff only area.**					

Use of digital and video images

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

- When using digital images, staff should inform and educate students / 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.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website / social media / local press

- 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 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.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The school / academy must ensure that:

- It has a Data Protection Policy in line with GDPR.
- It has paid the appropriate fee to the Information Commissioner's Office (ICO).
- It has appointed a Data Protection Officer (DPO).

- 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.
- Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice.
- Where special category data is processed, a lawful basis and a separate condition for processing have been identified.
- Data Protection Impact Assessments (DPIA) are carried out.
- It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.
- Procedures must be in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller.

- There are clear and understood Trust data retention policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.
- Consideration has been given to the protection of personal data when accessed using any remote access solutions.
- All academies (n.b. including Academies, which were previously exempt) must have a Freedom of Information Policy which sets out how it will deal with FOI requests.
- All staff receive data handling awareness / data protection training and are made aware of their responsibilities.

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.
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device 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 school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed

Communication Technologies	Staff & other adults				Pupils			
Mobile phones may be brought to the academy	x						x	
Use of mobile phones in lessons				x				x
Use of mobile phones in social time		x						x
Taking photos on mobile phones / cameras				x				x
Use of other mobile devices e.g. tablets, gaming devices		x						x
Use of personal email addresses in academy , or on school / academy network		x						x
Use of academy email for personal emails				x				x
Use of messaging apps		x						x
Use of social media		x						x
Use of blogs		x					x	

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 should therefore use only the academy email service to communicate with others when in school, or on academy systems.

- Users must immediately report, to the Head Teacher, 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, social media, chat, blogs, VLE 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.

- Whole class / group email addresses may be used at KS1, while pupils at KS2 and above will be provided with individual academy email addresses for educational use.

Social Media - Protecting Professional Identity

All schools, academies, MATs and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies, MATs and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the academy or local authority / MAT 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:

- Ensuring that personal information is not published
- Training is provided including acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions, as detailed in Acceptable Use Policy
- Risk assessment, including legal risk

School / 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 MAT
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the academy trust or impacts on the academy trust, it must be made clear that the member of staff is not communicating on behalf of the academy trust with an appropriate disclaimer. Such personal communications are within the scope of this policy

- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The academy permits reasonable and appropriate access to private social media sites

Dealing with unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from academy and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in an academy 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 an academy context and that users, as defined below, should not engage in these activities in / or outside the academy when using academy equipment or systems. The academy policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
Users shall not	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
	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	
	Promotion of extremism or terrorism				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 school / 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	

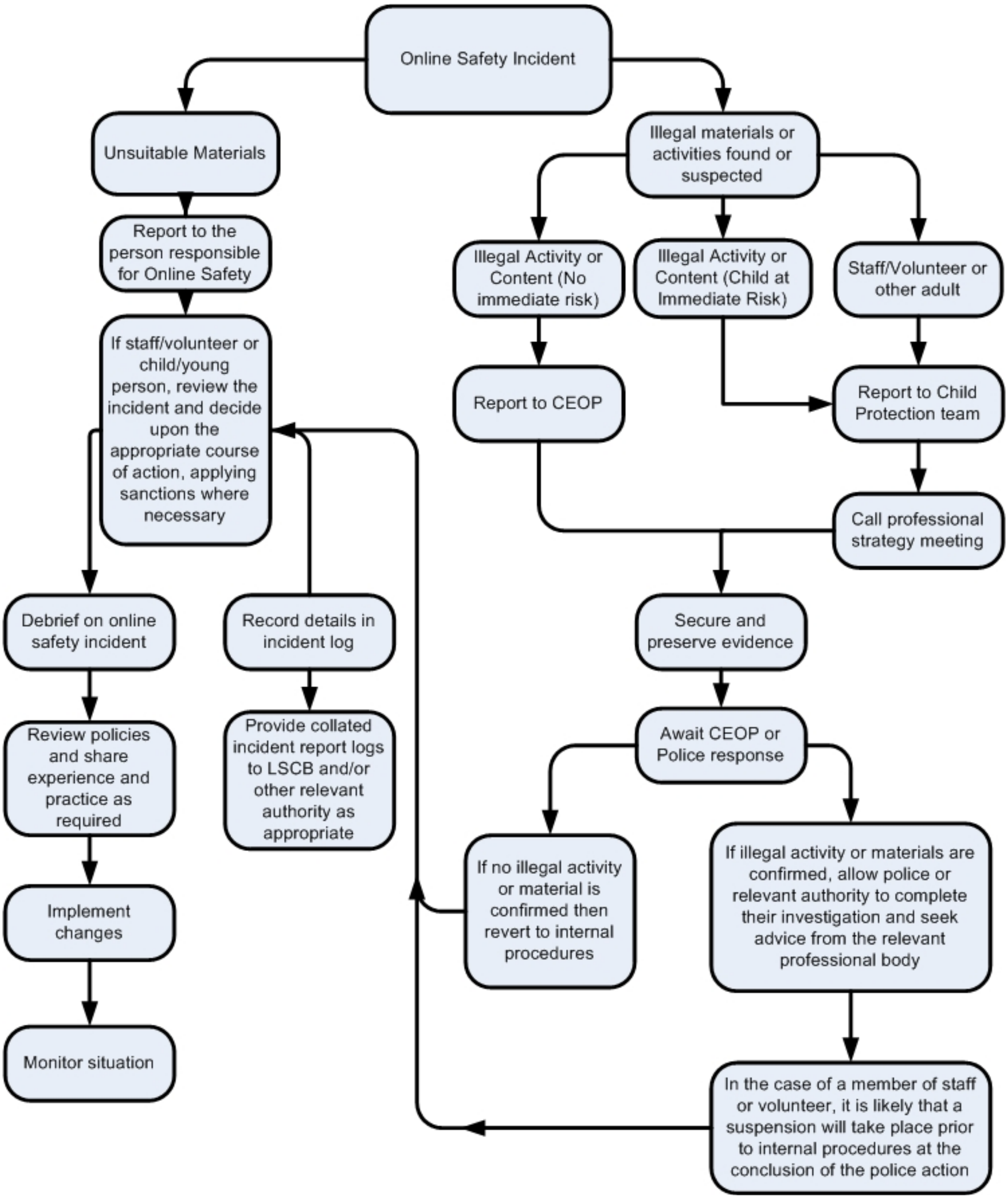
User Actions	Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)		x			
On-line gaming (non-educational)				X	
On-line gambling				X	
On-line shopping / commerce		X			
Secure 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 (below and appendix) for responding to online safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

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 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 Trust Board
    - 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

  - promotion of terrorism or extremism
  - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school / academy and possibly the police and demonstrate that visits to these sites were carried out for safeguarding 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 school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

1.

Students / Pupils Incidents		Refer to class teacher	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access	Warning	Further sanction eg detention /
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						x	
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device		x	x			x		x	X
Unauthorised / inappropriate use of social media / messaging apps / personal email		x	x			x		x	X
Unauthorised downloading or uploading of files		x	x		x	x		x	X
Allowing others to access school / academy network by sharing username and passwords		x				x		X	
Attempting to access or accessing the school / academy network, using another student's / pupil's account		x				x		x	X
Attempting to access or accessing the school / 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	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		x	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 / academy into disrepute or breach the integrity of the ethos of the school			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
Accidentally accessing offensive or pornographic material and failing to report the incident			x		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	

6.

Staff Incidents	Refer to Line Manager	Refer to Head Teacher	Refer to Trust Board	Refer to Police	Refer to Technical Support Staff for action re	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				
Inappropriate personal use of the internet / social media / personal email		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	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	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		x	x	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	x
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		x	x	x	x		x	x
Actions which could compromise the staff member's professional standing	x	x				x		

Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy	x	x			x	X	
Using proxy sites or other means to subvert the school's / academy's filtering system	x			x	X		
Accidentally accessing offensive or pornographic material and failing to report the incident	x	x		x	x	x	
Deliberately accessing or trying to access offensive or pornographic material	x	x	x	x		x	X
Breaching copyright or licensing regulations	x				X		
Continued infringements of the above, following previous warnings or sanctions	x	x				x	x

Pupil Acceptable Use Policy Agreement – Reception – Year 4
School Policy

To stay safe, when using ICT equipment, at our school:

- I will ask a teacher or suitable adult if I want to use ICT equipment such as ipads, computer etc.
- I will only access or use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of the computer and other equipment
- I will always ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will ask for help or tell a teacher or suitable adult if something appears that I wasn't expecting to see
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I will never share any personal information online, this includes my name, address and school
- I will not communicate or send messages with others online
- I will always tell an adult if someone tries to communicate with me
- I know that if I break the rules I might not be allowed to continue using the ICT equipment

Staff Acceptable Use Policy Agreement

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within 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 whilst 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 staff are protected from potential risk in their use of technology in their everyday work.

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

Acceptable Use Policy Agreement

I understand that I must use school 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 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. Members of staff should consult the school's online safety policy for further information and clarification.

For my professional and personal safety:

- I understand that the academy will monitor my use of the school digital technology and communications systems including my use of school information systems, Internet and email to ensure policy compliance.
- I understand that it is a civil offence to use a school ICT system for a purpose not permitted by its owner.
- 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 appreciate that ICT includes a wide range of systems, including I-pads, laptops, mobile phones, tablets, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that the school 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 report any incidents of concern regarding children’s safety to the Online Safety Coordinator, the Designated Child Protection Officer or Headteacher.
- I will promote online safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

I will be professional in my communications and actions when using 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 school's policy on the use of digital / video images. I will not use my personal equipment to record these images. Where these images are published (eg on the school website) it will not be possible to identify by name, or other personal information, those who are featured. Under no circumstances will I post photos outside of the school website.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils and parents/carers using official school 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 school and the local authority 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 and will ensure that 3G/4G data access is turned off when in school.
- 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, in accordance with relevant academy policies.
- 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 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, remove hardware or software or factory re-set any device
- 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 Academy Data Protection Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by 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 will ensure that all devices are returned to the school immediately, if requested, and that they are not for my personal use

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

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

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

- I understand that this Acceptable Use Policy applies not only to my work and use of academy digital technology equipment in school, but also applies to my use of 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 the ADC / Trust Board and / or the Local Authority and in the event of illegal activities the involvement of the police.
- I understand that the academy will exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

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

Signature: ……………………………Printed……………………………………

Date: …………………………………

Accepted for school: …………………………Printed:……………………………

Date: …………………………………

ß

Volunteers Acceptable Use Policy Agreement

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within 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 whilst 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 staff are protected from potential risk in their use of technology in their everyday work.

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

Acceptable Use Policy Agreement

I understand that I must use school 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 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. Members of staff should consult the school's online safety policy for further information and clarification.

For my professional and personal safety:

- I understand that the academy will monitor my use of the school digital technology and communications systems including my use of school information systems, Internet and email to ensure policy compliance.
- I understand that it is a civil offence to use a school ICT system for a purpose not permitted by its owner.
- 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 appreciate that ICT includes a wide range of systems, including I-pads, laptops, mobile phones, tablets, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that the school 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 report any incidents of concern regarding children's safety to the Online Safety Coordinator, the Designated Child Protection Officer or Headteacher.
- I will promote online safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

I will be professional in my communications and actions when using 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 school's policy on the use of digital / video images. I will not use my personal equipment to record these images.

Where these images are published (eg on the school website) it will not be possible to identify by name, or other personal information, those who are featured. Under no circumstances will I post photos outside of the school website.

- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils and parents/carers using official school 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 school and the local authority 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 and will ensure that 3G/4G data access is turned off when in school.
- 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, in accordance with relevant academy policies.
- 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 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, remove hardware or software or factory re-set any device
- 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 Academy Data Protection Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by 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 will ensure that all devices are returned to the school immediately, if requested, and that they are not for my personal use

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

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

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

- I understand that this Acceptable Use Policy applies not only to my work and use of academy digital technology equipment in school, but also applies to my use of 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 the LGB / Trust Board and / or the Local Authority and in the event of illegal activities the involvement of the police.

- I understand that the academy will exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

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

Signature: …………………………………Printed:……………………………………

Date: …………………………………

Accepted for school: …………………………Printed: ………………………….……

Date: …………………………………