Nourishing the fitrah of each unique child

Online Safety Policy

"Verily! The hearing, the sight and the heart, of each of those you will be questioned."
(Surah Al- Isra, The Night Journey, Verse: 36)

Adopted: **January 2024**	**Review date:** **January 2025**	**Online Safety Coordinator:** **Sanaa Arshad**

Adopted: January 2024 Reviewed: January 2025

Online Safety Policy

Contents

Online Safety Policy Overview

Online Safety is part of the wider safeguarding and protection procedures and Unique Academy it is our duty to ensure that every child is safe by promoting healthy and safe use of the internet. This policy document is drawn up to protect all parties – the pupils, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Unique Academy with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff.
- Assist school staff working with children to work safely and responsibly with the Internet and other IT and communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use for the whole school community.
- Have clear structures to deal with online abuse such as online bullying.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

The main areas of risk for our school community can be summarised as follows:

- Content and Conduct
- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content
- Contact
- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords
- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Copyright (little care or consideration for intellectual property and ownership)

Scope

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

Roles and Responsibilities

Role	Key Responsibilities
Safeguarding Trustee (including online safety)	• To ensure that the school has in place policies and practices to keep the children and staff safe online • To approve the Online Safety Policy and review the effectiveness of the policy annually • To support the school in encouraging parents and the wider community to become engaged in online safety activities
Headteacher	• Must be adequately trained in online safeguarding • To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding. • To take overall responsibility for online safety provision • To take overall responsibility for data management and information security ensuring school's provision follows best practice in information handling • Ensure that online safety education is embedded within the curriculum • To ensure the school uses appropriate IT systems and services including, filtered Internet Service • To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety • Report to CEOP or IWP if where there is suspect of grooming or sexual exploitation • Ensure suitable 'risk assessments' undertaken so the curriculum meets needs of pupils, including risk of children being radicalised • To conduct audits and receive regular monitoring feedback from the Online Safety Co- ordinator • To ensure trustees are regularly updated on the nature and effectiveness of the school's arrangements for online safety • To ensure the school website includes relevant information.

Role	Key Responsibilities
Online Safety Co-ordinator	• Take day to day responsibility for online safety issues • Promote an awareness and commitment to online safety throughout the school community • To communicate regularly with SLT to discuss current issues, review incident logs and filtering/change control logs • To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident • To ensure that online safety incidents are logged as a safeguarding

	incident ● Oversee any parents surveys / feedback on online safety issues ● Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection concerns. ● To ensure that the data they manage is accurate and up-to-date ● Ensure best practice in information management. i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements.
Teachers	● To embed online safety in the curriculum ● To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) ● To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws ● Run off mobile phones while at school and keep away from the classroom, only communicate with parents, using the school's equipment ● Do not communicate with parents or teachers outside school.
All staff, volunteers and contractors.	● To adhere to the school staff Acceptable Use Agreement ● To report any suspected misuse or problem to the online safety coordinator ● To maintain an awareness of current online safety issues and guidance e.g. through CPD ● To model safe, responsible and professional behaviours in their own use of technology ● PSHE policy to teach pupils about misinformation and fake news **Exit strategy** ● At the end of the period of employment/volunteering to return any equipment or devices loaned by the school. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with line manager on the last day to log in and allow a factory reset.

Role	Key Responsibilities
Pupils	● To the Pupil Acceptable Use Policy ● To understand the importance of reporting abuse, misuse or access to inappropriate materials ● To know what action to take if they or someone they know feels worried or vulnerable when using online technology ● To understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school ● To contribute to any 'pupil voice' / surveys that gathers information of their online experiences
Parents/carers	● To read, understand and promote the school's Pupil Acceptable Use Agreement with their child/ren ● to consult with the school if they have any concerns about their children's use of technology ● to support the school in promoting online safety and agree to their children's use of the Internet at school and the school's use of photographic and video images ● Promote e-safety awareness through newsletters and informal meetings ● Advocate the computer be placed in the main family room at home ● Install filtering at home and set clear boundaries
External groups including Parent groups	● Any external individual/organisation will read and agree to an Acceptable Use Policy prior to using technology or the Internet within school ● to support the school in promoting online safety ● To model safe, responsible and positive behaviours in their own use of technology.

Communication

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website as well as made available on the 'school' shared drive.
- Regular updates and training on online safety for all staff.
- Acceptable use agreements discussed with staff and pupils. Acceptable use agreements to be issued to the whole school community, on entry to the school.

Handling Incidents

- The school will take all reasonable precautions to ensure online safety.
- Staff and pupils will be given information about infringements in use and possible sanctions.
- Online Safety Coordinator (School Administrator) acts as the first point of contact for any incident.
- Any suspected online risk or infringement is reported to Online Safety Coordinator that day any concern about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Safeguarding Trustee.

Education and Curriculum

Pupil online safety curriculum

Unique Academy:

- has a clear, progressive online safety education curriculum as part of our Computing curriculum. This covers a range of skills and behaviours appropriate to their age and experience;
- plans online use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- will remind pupils about their responsibilities through the pupil Acceptable Use Agreements;
- ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright;
- ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
- ensure pupils only use school-approved systems and publish within appropriately secure / age-appropriate environments.
- Children will understand how to keep themselves self while using technology

Staff Training

Unique Academy:

- makes regular training available to staff on online safety issues and the school's online safety education program;
- provides, as part of the induction process, all new staff with information and guidance on the Online Safety Policy and the school's Acceptable Use Agreements.

Parent Awareness And Training

Unique Academy will:

- make this policy available on its website, including in hard copy if requested.
- provide online safety information, advice, guidance and training for parents.

Radicalisation and the Use of Social Media to Encourage Extremism

The internet and the use of social media in particular has become a major way to communicate with others, especially young people, which has provided access for like-minded people to create an online community and confirm extreme beliefs such as extreme ideological views or the use of violence to solve problems.

This has led to social media becoming a platform for:

- intensifying and accelerating the radicalisation of young people
- confirming extreme beliefs
- accessing to like minded people where they are not able to do this off-line, creating an online community
- normalising abnormal views and behaviours, such as extreme ideological views or the use of violence to solve problems and address grievances.

Unique Academy has a number of measures in place to help prevent the use of Social Media for this purpose:

- Web site filtering is in place to help prevent access to terrorist and extremist material and social networking sites such as Facebook, Instagram or Twitter by Pupils
- Pupils, Parents and Staff are educated in safe use of Social Media and the risks posed by on-line activity, including from extremist and terrorist groups.

Further details on how social media is used to promote extremism and radicalisation can be found in guidance from the Department for Education.

Reporting of e-Safety issues and concerns including concerns regarding Radicalisation

Our Designated Safeguarding Lead provides advice and support to other members of staff on protecting children from the risk of on-line radicalisation. Unique Academy ensures staff understand what radicalisation and extremism mean and why people may be vulnerable to being drawn into terrorism.

We ensure staff have the knowledge and confidence to identify children at risk of being drawn into terrorism, and to challenge extremist ideas which can be used to legitimise terrorism. Staff safeguard and promote the welfare of children and know where and how to refer children and young people for further help as appropriate by making referrals as necessary to Channel.

Assessing Risks:

- We will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of Internet access.
- Emerging technologies, such as mobile phones with internet access (smartphones) are not governed by the school's infrastructure and bypass all security and filtering measures that are or could be deployed.
- We will audit ICT use to establish if the Online Safety policy is sufficiently robust and that the implementation of the e-safety policy is appropriate and effective.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- Emerging technologies will be examined by the Head teacher for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Any person not directly employed by the school will not be provided with access to any of the school systems with the exception of filtered Wi-Fi access.

Cyber-Bullying

Cyberbullying is bullying using technology to threaten, embarrass or cause discomfort. Seven categories of cyberbullying have been identified:

- Text message bullying involves sending unwelcome texts
- Picture/video-clip bullying via mobile phone cameras with images or video clips usually sent to other people.
- Phone call bullying via mobile phone uses silent calls or abusive messages. Sometimes the bullied person's phone is stolen and used to harass others, who then think the phone owner is responsible.
- Email bullying often uses a pseudonym for anonymity or using someone else's name to pin the blame on them.
- Online grooming, Chat room and Social Networking Site abuse involves sending menacing or upsetting

responses to pupils or young people.

- Bullying through instant messaging (IM) is an Internet-based form of bullying where pupils and young people are sent unpleasant messages as they conduct real-time conversations online
- Bullying via websites includes the use of defamatory blogs (web logs), personal websites and online personal polling sites.

There has also been a significant increase in social networking sites for young people, which can provide new opportunities for cyber-bullying.

ICT Based Sexual Abuse

The impact on a child of ICT based sexual abuse is similar to that for all sexually abused pupils. However, it has an additional dimension in that there is a visual record of the abuse. ICT based sexual abuse of a child constitutes significant harm through sexual and emotional abuse. Recognition and response is recognising a situation where a child is suffering, or is likely to suffer a degree of physical, sexual and/or emotional harm (through abuse or neglect) which is so harmful that there needs to be compulsory intervention by child protection agencies into the life of the child and their family. All adults (volunteers, staff) working with pupils, adults and families will be alerted to the possibility that:

- A child may already have been/is being abused and the images distributed on the internet or by mobile telephone
- An adult or older child may be grooming a child for sexual abuse, including involvement in making abusive images. This process can involve the child being shown abusive images
- An adult or older child may be viewing and downloading child sexual abuse images.

Chat Room Grooming and Offline Abuse

Our staff will need to be continually alert to any suspicious activity involving computers and the Internet. Grooming of pupils online is a faster process than usual grooming, and totally anonymous. The abuser develops a 'special' relationship with the child online (often adopting a false identity), which remains a secret to enable an offline meeting to occur in order for the abuser to harm the child.

Expected Conduct and Incident Management

Expected conduct

At Unique Academy, all users:

- are responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Agreements;
- understand the significance of misuse or access to inappropriate materials and are aware of the consequences;
- understand it is essential to reporting abuse, misuse or access to inappropriate materials and know how to do so;
- understand the importance of adopting good online safety practice when using digital technologies in and out of school;
- be mindful who they follow on social media
- Be mindful of what you download and share
- Be careful of what you post
- know and understand school policies on the use of mobile and handheld devices including cameras
- consider digital footprint- linked with Halaqah;

Staff, volunteers and contractors:

- know to be vigilant in the supervision of children at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- know to take professional, reasonable precautions when working with pupils, previewing websites before use; using age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils; Parents/Carers:
- should know and understand what the school's 'rules of appropriate use for the whole school community' are and what sanctions result from misuse.
- should monitor their child's use of online learning in the event of remote education.

Incident Management

At Unique Academy:

- there is strict monitoring of the online safety policy and a differentiated and appropriate range of sanctions;
- all members of the school are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes;

- support is actively sought from other agencies as needed (i.e. UK Safer Internet Centre helpline, Local authority Prevent Officer, Police etc) in dealing with online safety issues;
- monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school;
- parents/carers are specifically informed of online safety incidents involving children for whom they are responsible;
- the Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law;
- we will immediately refer any suspected illegal material to the appropriate authorities – i.e. Police etc.

Managing IT and Communication System

Internet access, security (virus protection) and filtering (see Appendix 1)

Unique Academy:

- informs all users that Internet/email use is monitored;
- has the educational filtered secure broadband connectivity;
- uses a filtering system which blocks sites that fall into categories (e.g. adult content, race hate, gaming). All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status;
- ensures network health through use of Norton anti-virus software on any Windows computers;
- Uses approved systems and password protecting documents when emailing to send 'protect-level' (sensitive personal) data over the Internet
- Uses encrypted devices (staff iPads are encrypted and password protected) or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site;
- Ensures that any concerns about the system are communicated so that systems remain robust and protect pupils.

Network management (user access, backup)

Unique Academy:

- Uses individual, audited log-ins for all users for staff using desktop computers and with pupils when they set up their 1:1 assigned tablet;
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services;
- Has daily back-up of school data (admin and curriculum);
- Uses secure, 'Cloud' storage for data back-up
- Storage of all data within the school will conform to the EU and UK data protection requirements; Storage of data online, will conform to the EU data protection directive where storage is hosted within the EU.

To ensure the network is used safely, Unique Academy:

- Ensures staff read and understand the school's online safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. The same credentials are used to access the school's network.
- Has set-up the network with multiple shared work areas for admin staff and teaching staff. Pupils have no access to this resource;
- Requires all users to log off when they have finished working or lock the screen when they are leaving the computer unattended;
- Makes clear that staff are responsible for ensuring that any computer (PC or tablet) loaned to them by the school, is used primarily to support their professional responsibilities.
- Maintains equipment to ensure Health and Safety is followed;
- Ensures that access to the school's network resources from remote locations by staff is audited and restricted and access is only through school approved systems:
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is audited restricted and is only through approved systems;
- Has a clear system in place that includes a secure, remote offsite backup of data on Google drive;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our secure file exchange
- All IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards.

Password Policy

- Unique Academy makes it clear that staff and pupils must always keep their passwords private,and not share with others; If a password is compromised the school should be notified immediately.
- All staff have their class username and private passwords to access school systems. Staff are responsible for keeping their passwords private.
- We require staff to use strong passwords.
- We require staff using critical systems to use two factor authentication.

E-mail

Unique Academy:

- Provides staff with an email account for their professional use
- Will contact the Police if one of our staff or pupils receives an email that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date
- We use a number of technologies to help protect users and systems in the school, including desktop anti-virus product Norton for Windows PCs, plus direct email filtering for viruses.

Pupils:

- Pupils are taught about the online safety and 'netiquette' of using e-mail both in school and at home. Staff:
- Staff can only use the school email systems on the school system
- Staff will use the school e-mail systems for professional purposes
- If staff or pupil personal data is transferred by email, it must be password protected first.

School Website

- The Headteacher, supported by the Trustees, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Photographs published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website

Cloud Environments

- Uploading of information on the schools' online learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas;
- Photographs and videos uploaded to the school's online environment will only be accessible by members of the school community
- In school, pupils are only able to upload and publish within school approved 'Cloud' systems.

Social Networking

Staff, Volunteers and Contractors:

- Staff are instructed to always keep professional and private communication separate.
- Teachers are instructed not to run social network spaces for pupil use on a personal basis or to open up their own spaces to their pupils, but to use the schools' preferred system for such communications.

Unique Academy staff will ensure that in private use:

- No reference should be made in social media to pupils, parents/carers or school staff;
- School staff should not be online friends with any pupil.
- 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 school and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute;
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Pupils:

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- Pupils are required to follow our pupil Acceptable Use Agreement.

Parents:

- Parents are reminded about social networking risks and protocols through parent workshops on Online Safety and additional communications materials when required.
- Must not upload videos or photos that include other people's children to social media.

CCTV

- We have CCTV in the school as part of our site surveillance for staff and student safety. The use of CCTV is clearly signposted in the school. We will not reveal any recordings without appropriate permission.
- We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use them for any other purposes.

Data Security: Management Information System Access and Data transfer

Strategic and operational practices

At Unique Academy:

- Staff are clear who the key contact(s) for key school information are.
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in a single central record.

Technical Solutions

- Staff have secure areas on the network to store sensitive files.
- We require staff to log-out or lock the screen of systems when leaving their computer.
- We use Business Talk Talk for access to broadband services
- Details of all school-owned hardware will be recorded in a hardware inventory.
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.
- Where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data.

Equipment and Digital Content

Mobile Devices (Mobile phones, tablets and other mobile devices)

- Mobile devices brought into school are entirely at the staff member, pupils & parents or visitors' own risk. The School accepts no responsibility for the loss, theft or damage of any phone or handheld device brought into school.
- Pupils are not permitted to bring in their own mobile phone to school under any circumstances.
- Staff and pupils are given access to school-owned mobile devices (Tablets etc). These are the only devices to be used during lesson time.
- Videos and images should only be taken on mobile devices that the school owns. The consent of the people or person involved must always be sought.
- Staff members may not use their mobile phones at all during the school day.
- All visitors are requested to keep their phones on silent and not use them when around children.
- The School reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying. This includes school-assigned and personal devices.

Storage, Synching and Access

- Teaching staff will be provided with a school email address.
- Teachers are permitted to download apps from the App Store that may be useful for teaching and learning.
- Tablets will be passcode protected by the school administrator and these passcodes will be shared with teachers

Pupils' use of personal devices

- Pupil mobile phones and devices must not be brought into school.
- If a pupil's mobile phone is found at any other time, it will be confiscated and will be held in a secure place in the school office until the end of the day.

Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices in a professional capacity, such as for contacting children, young people or their families whilst at school (refer to Mobile policy).
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.

- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes and then report the incident with the Headteacher.
- If a member of staff breaches the school policy then disciplinary action may be taken.

Digital images and video

In this school:

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their child joins the school;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials;
- We share the schools Acceptable Use Policy with staff and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils;
- The school blocks/filter access to social networking sites unless there is a specific approved educational purpose;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Reviewing and Monitoring Online Safety

The online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school.

Staying Safe During Home Learning

At Unique Academy we understand that we have a duty to maintain the rights of children in providing effective learning which will continue to stimulate and motivate children. We recognise that during home learning, children are greater at risk of abuse such as bullying, trolling and grooming as well as developing emotional issues.

Parents and children will be reminded to take similar precautions during home learning and will maintain the

hours of learning agreed by the school and communicate through the school channels and be active participants in the children's learning.

During online lessons, parents of early years, will be advised to be present during lessons, as this will better aid their learning and concentration.

We aim to provide emotional support for parents and children during this time and parents will be advised to:

- Talk to their children about On-line safety and have parental control of devices
- Be aware of children's on-line friends
- Provide a suitable space for learning
- Avoid digital devices in children's bedroom as these disrupts the quality of sleep
- Monitor online activities and access to mobile phones, laptops and games console
- Limit access to websites and Apps
- Be alert to sudden changes in moods and behaviour and contact the school with any concerns

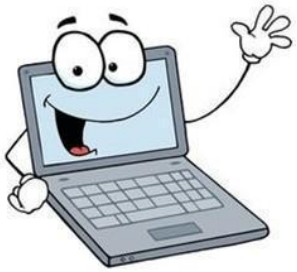
Pupil Acceptable Use Policy Agreement for pupils

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers / tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer /tablet

Signed (child): ....._____

Signed(parent): ....._____



Parent / Carer Acceptable Use Agreement

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 pupils will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school 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 online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Pupil 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 are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Parent / Carer Permission Form

Parent/Carers Name: _____

Pupil Name: _____

As the parent / carer of the above *pupils*, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

I understand that the school has discussed the Acceptable Use Agreement with my son/daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Signed: .._____

Date: .._____

Use of Digital /Video Images

The use of digital / video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of 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 school website and occasionally in the public media.

The school 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 that the children cannot be identified by their faces or by the use of their names.

In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos of their own children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the video image.

Parents / carers are requested to sign the permission form below to allow the school to take and use images (without faces) of their children and for the parents / carers to agree.

Digital / Video Images Permission Form

Parent/CarersName: .._____

Pupil Name: _____

As the parent / carer of the above pupil, I agree to the school taking and using digital / video images of my child / children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.	Yes / No
I agree that if I take digital or video images at, or of – school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.	Yes / No

Signed: .....

Date: .....

Staff (and Volunteer) Acceptable Use Policy Agreement

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

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school 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 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 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.

For my professional and personal safety:

- I understand that the *school* will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- 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 be professional in my communications and actions when using *school ICT* systems:

I will not access, copy, remove or otherwise alter any other user's files, without their express permission.

I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.

I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.

I will only communicate with students / pupils and parents / carers using official 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 has a responsibility to provide safe and secure access to technologies and ensure the smooth running of the *school*:

When I use my mobile devices (laptops / tablets / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using *school* equipment. I will also follow any additional rules set by the *school* about such use. I will ensure that any such devices are protected by up to date anti- virus software and are free from viruses.

I will not use personal email addresses on the school ICT systems unless permission is granted.

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 school 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 (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 school policies.

I will not disable or cause any damage to school equipment, or the equipment belonging to others.

I will only transport, hold, disclose or share personal information about myself or others, as outlined in the school data protection policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and restricted data must be held in lockable storage.

I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.

I will immediately report any damage or faults involving equipment or software, however this may have happened.

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

I will ensure that I have permission to use the original work of others in my own work

Where work is protected by copyright, I will not download or distribute copies (including music and videos).

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

I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school

I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include suspension or loss of job. A warning, a suspension, referral to the Trustees and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school 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.

Staff / VolunteerName:_____

Signed: .._____

Date ……..

Unique Academy Online Safety Incident Reporting Form

Details of person reporting the incident Name: Phone number: Email address:
Date of incident:
Where did the incident take place?
Description of the incident
Name(s) of those involved in the incident:
Age(s) of child(ren) involved:

Was the incident				
Child on adult☐	Child on child☐	Staff member on child☐	Adult on child☐	Adult on adult☐

Type of incident					
Sexual ☐	Profanity☐	Bullying☐	Violence☐	Grooming☐	Other☐

Please give details:

How was the content accessed?							
mobile phone using an alternative provider ☐	School internet via a PC/laptop ☐	Tablet using alternative provider ☐	Via an internet browser ☐	via a social media website ☐	via a mobile phone ☐	via email☐	via an app ☐
What action was taken in relation to those involved in the incident?							
What action was taken regarding the site/content accessed?							

What follow up action was taken?		
Referral to LADO ☐	Referral to Children's Social Care ☐	Advice to parents☐
Police investigation ☐	Referral to Trustees ☐	Other ☐
Please provide details:		

Record of reviewing devices / internet sites (responding to incidents of misuse)

Group: _____

Date: _____

Reason for investigation: _____

.....

.....

.....

Details of first reviewing person

Name: _____

Position: _____

Signature: _____

Details of second reviewing person

Name: _____

Position: _____

Signature: _____

Name and location of computer used for review (for web sites)

.....

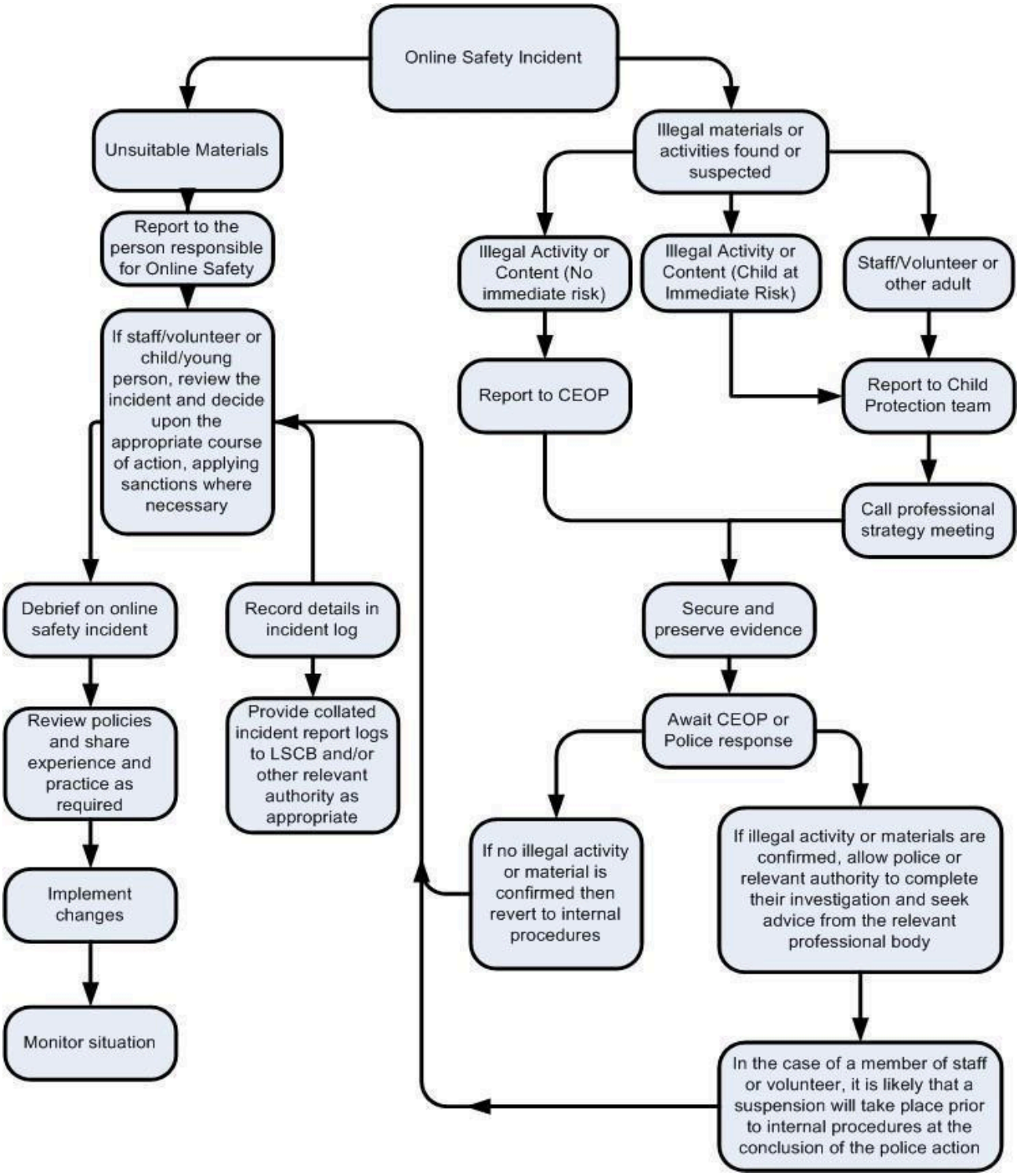
.....

Web site(s) address / device	Reason for concern

Conclusion and Action proposed or taken

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.



APPENDIX 1:

Unique Academy Web Filtering

The internet package with TalkTalk Business is called Worksafe. Below are the services it offers:

WorkSafe Services:

- Stop Misuse
The Stop Misuse feature allows the head teacher to choose from a range of website categories to block, such as unapproved file sharing sites. The head teacher can also block or allow specific websites in a few simple steps.

- Business Hours
Unique Academy staff are prevented from getting distracted during office hours by choosing when to block for example, social media and gaming websites.

- Virus Protection Alerts
Unique Academy staff and pupils are protected from viruses and other threats. All users connected to the school's office Wi-Fi will be prompted with a warning pop up if they visit a suspicious website.

- HTTPS blocking
The ability to prevent HTTPS traffic means less risk for Unique Academy, as it filters even more possible URLs and results.

The internet blocking functions prevent:

Drugs, Tobacco and Alcohol: Websites that promote either the legal or illegal use, manufacture or distribution of drugs, alcohol and tobacco.

Dating: Websites which introduce people to others online looking for relationships, for example www.plentyoffish.com, www.match.com

Gambling: Websites where people can place bets/gamble (includes lotteries), for example www.888.com, www.betfair.com.

Pornography: Websites that contain sexually explicit material.

Violence & Weapons: Websites that promote violence, weapons and the infliction of pain.