E-Safety Policy

Author	Liane Johnson
Approved by Governing Body	November 2022
Review Date	November 2023
First Version Date	November 2016
Version	V5

E Safety Policy

This policy should be viewed alongside the following school policies which have relevance to safeguarding:

- Safeguarding and Child Protection
- Whistleblowing Policy
- Staff Code of Conduct
- Allegations Against Adults Policy
- Data Protection
- Data security
- Low Level Concerns Policy

It is written with reference to the following key documents and statutory guidance:

- *Keeping Children Safe in Education 2021*
- *Working Together to Safeguard Children 2018*
- *Prevent Duty Guidance 2015*
- *The Prevent Duty; Departmental advice for schools and childcare providers 2015*
- Guidance for safer working practice for adults who work with children and young people in education settings 2019

Responsibilities

The member of staff responsible for e-safety is Amanda Brown

They are responsible for delivering staff development and training, recording incidents, reporting any developments and incidents and liaising with the local authority and external agencies to promote e-safety within the school community. She may also be required to deliver workshops for parents.

Internet use and Acceptable Use Policies (AUPs)

All members of the school community should agree to an Acceptable Use Policy that is appropriate to their role.

Examples of the AUPS used can be found in appendix 1.

The children at Nursery school are deemed to be too young to complete an AUP.

AUP's will be reviewed annually. All AUPs will be stored centrally in case of breaches of the e-safety policy.

The Prevent Duty

The Prevent Duty is the duty in the Counter-Terrorism and Security Act 2015 on specified authorities (Schools) in the exercise of their functions, to have due regard to the need to prevent people from being drawn into terrorism.

The general risks affecting children and young people may vary from area to area, and according to their age. Schools and childcare providers are in an important position to identify risks within a given local context.

Schools and childcare providers should be aware of the increased risk of online radicalisation, as organisations seek to radicalise young people through the use of social media and the internet.

The statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. Schools should ensure that suitable filtering is in place. For Aspiring Foundations Federated Nursery Schools this is provided via Halton BC service level agreement.

More generally, schools have an important role to play in equipping children and young people to stay safe online, both in school and outside. General advice and resources for schools on internet safety are available on the UK Safer Internet Centre website. As with other online risks of harm, all staff need to be aware of the risks posed by the online activity of extremist and terrorist groups.

The Prevent Duty means that all staff have a duty to be vigilant and where necessary report concerns over use of the internet that includes, for example, the following:

- Internet searches for terms related to extremism
- Visits to extremist websites
- Use of social media to read or post extremist material
- Grooming of individuals

The Prevent Duty requires a schools monitoring and filtering systems to be fit for purpose. For Aspiring Foundations Federated Nursery Schools these are provided via Halton BC service level agreement.

Photographs and Video

The use of photographs and videos is popular in teaching and learning and should be encouraged. However, it is important that consent from parents is gained if videos or photos of pupils are going to be used.

If photos/videos are to be used online then names of pupils should not be linked to pupils.

Staff must be fully aware of the consent form responses from parents when considering use of images. This is updated annually as part of the data collection exercise.

Staff should always use a school camera to capture images and should not use their personal devices.

Children are deemed to be too young to be at risk to any exploitation arising from ‘upskirting’. Where children use mobile devices to take photographs around the provision they are always supervised by an adult. Mobile devices are not allowed into the bathroom areas. Mobile devices are only used online by children in the presence of an adult. They also covered by web filtering.

Photos taken by the school are subject to the Data Protection Act.

Photos and videos taken by parents/carers.

Parents and carers are permitted to take photos/videos of their own children in school events / on school visits. They are requested not to share photos/videos from school events on social networking sites if other pupils appear in the background.

Parents attending school based events will be reminded of their responsibilities in relation to social media verbally and through notices.

Photos for personal use such as those taken by parents/carers are not subject to the Data Protection Act.

Mobile phones and other devices

Aspiring Foundations Federated Nursery Schools recognise that there may be occasions when staff need to have access to mobile phones during the working day. However, there have been a number of queries raised within the local authority and nationally regarding the use of mobile phones and other devices in educational settings.

The concerns are mainly based around these issues:

- Staff being distracted from their work with children
- The use of mobile phones around children
- The inappropriate use of mobile phones

Ensuring the Safe and Appropriate Use of Mobile Phones

- Aspiring Foundations Federated Nursery Schools allow staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device.
- The use of mobile phones and similar devices whilst on duty within the childcare environment is strictly forbidden
- Staff must ensure that personal mobile phones are not carried about their person during working hours.
- Personal mobile phones must be kept in lockers provided during working hours, although can be used during lunch breaks.
- Using a mobile phone to take pictures or video clips of children is not allowed
- Where trips are taken outside of the school staff may use a personal mobile, which is fully charged and switched on for the duration of the trip. This number is recorded on the Evolve form and employees are reimbursed for any use associated with the trip accordingly. The phone cannot be used for taking photographs.

If staff fail to follow this guidance, disciplinary action will be taken in accordance to the school's staff code of conduct. If staff need to make an emergency call, they must do so either in the main or Headteacher's office. Staff must ensure that there is no inappropriate or illegal content on the device.

Mobile phone technology may not be used to take photographs anywhere within the school grounds. There are digital cameras and tablets available within the nursery/school and only these should be used to record visual information within the consent criteria guidelines of the local authority and the school.

Children should not use mobile phones within the school grounds and should not bring in a mobile to school at any time.

Use of Mobile Phones for Volunteers and Visitors

Upon their initial visit volunteers and visitors are given information informing them they are not permitted to use mobile phones on the premises. If they wish to make or take an emergency call they may use either the main or the manager's office. Neither are volunteers or visitors permitted to take

photographs or recordings of the children without the Headteacher's permission.

Important contact details of the children are kept in the office. In case of an emergency contact with a parent is made via the school office. This includes any contact that may need to be made with a parent whilst children are on an educational visit.

We believe that photographs validate children's experiences and achievements and are a valuable way of recording milestones in a child's life. Parental permission for the different ways in which we use photographs is gained as part of the initial registration at this school. We take a mixture of photos that reflect the pre-school environment; sometimes this will be when children are engrossed in an activity either on their own or with their peers. Children are encouraged to use the camera to take photos of their peers. In order to safeguard children and adults and to maintain privacy, cameras are not to be taken into the toilets by adults or children. All adults whether teachers/practitioners or volunteers at the school understand the difference between appropriate and inappropriate sharing of images.

All images are kept securely in compliance with the Data Protection Act.

If a member of staff suspects that a mobile phone has been misused within the school then it should be confiscated but staff should not 'search' the phone. The incident should be passed directly to SLT who will deal the matter in line with normal school procedures.

Use of e-mails
The E-mail system should only be used for school related matters. Staff are advised to maintain an alternative personal e-mail address for use at home in non-school related matters.

Security and passwords
Passwords should be changed regularly. The system will inform users when the password is to be changed. Passwords must not be shared. Staff must always 'lock' the PC if they are going to leave it unattended (the picture mute or picture freeze option on a projector will allow an image to remain on the screen and also allow a PC to be 'locked').
All users should be aware that the ICT system is filtered and monitored.

Data storage
Only encrypted USB pens are to be used in school.

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 school/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 a school context, either because of the age of the users or the nature of those activities**.**

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

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

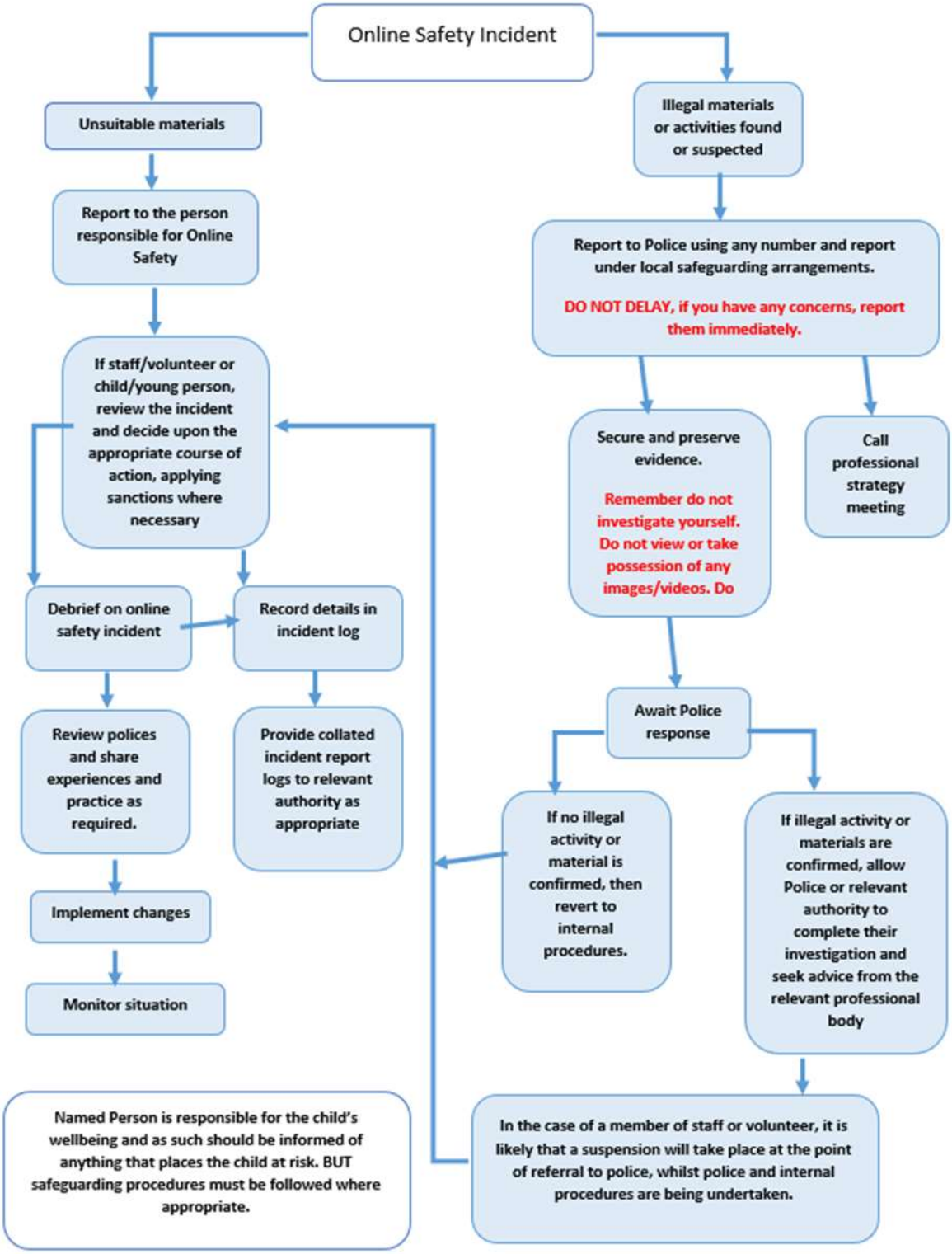
User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978 N.B. Schools/academies should refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	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	
Activities that might be classed as cyber-crime under the Computer Misuse Act: • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices						X

• Using penetration testing equipment (without relevant permission) N.B. We take the view these type of offences would be classed as Cyber Crime and a deliberate attack on the security of the Federation and therefore we would seek further support from the LA and the police. Serious or repeat offences would be reported to the police.					
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school/academy				X	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)				X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				X	
Using school systems to run a private business				X	
Infringing copyright				X	
On-line gaming (educational)				X	
On-line gaming (non-educational)				X	
On-line gambling				X	
On-line shopping/commerce				X	
File sharing		X			
Use of social media			X		
Use of messaging apps			X		
Use of video broadcasting e.g. Youtube		X			

Responding to incidents of misuse

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

Illegal Incidents
If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (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
Record details in incident log
Review polices and share experiences and practice as required.
Provide collated incident report logs to relevant authority as appropriate
Implement changes
Monitor situation
Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.
Illegal materials or activities found or suspected
Report to Police using any number and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself. Do not view or take possession of any images/videos. Do
Call professional strategy meeting
Await 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 at the point of referral to police, whilst police and internal procedures are being undertaken.

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow Federation 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 children 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 –appendix 6 (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority
    - 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
    - offences under the Computer Misuse Act (see User Actions chart above)
    - 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 *Federation* 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.

School actions & sanctions

It is more likely that the Federation 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:

Actions/Sanctions

Staff Incidents	Refer to line manager	Refer to Headteacher	Refer to Local Authority/HR	Refer to Police	Refer to Technical Support Staff for action re filtering	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		X	X	X				
Inappropriate personal use of the internet/social media/personal email		X				X		X
Unauthorised downloading or uploading of files		X			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
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X					X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X					X
Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with students/pupils		X						X
Actions which could compromise the staff member's professional standing		X				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		X
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X		X	X		
Deliberately accessing or trying to access offensive or pornographic material		X	X		X			X
Breaching copyright or licensing regulations		X	X		X			X
Continued infringements of the above, following previous warnings or sanctions		X	X					X

Social networking

Pupils are not permitted to use social networking sites within school.

E-Safety Education
Pupils

Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the eSafety curriculum.

Staff

a). A planned programme of formal e-safety training is made available to all staff. Additionally, all staff will have CPD on the Prevent duty.
b). E-safety training is an integral part of Child Protection / Safeguarding training and vice versa
c). All staff have an up to date awareness of e-safety matters, the current school e-safety policy and practices and child protection / safeguarding procedures
d). All new staff receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policy
e). The culture of the school ensures that staff support each other in sharing knowledge and good practice about e-safety
f). The school takes every opportunity to research and understand good practice that is taking place in other schools
g). Governors are offered the opportunity to undertake training.
h). Any staff member who is concerned re e safety or wants further advice re apps / online bullying or harassment also access free advice re the Professional on line safety help line 0344 381 4772; helpline@saferinternet.org.uk

Parents and the wider community

Parents are also supported to start to develop good habits re E safety at home and to learn about family safety planning. This is offered as part of the Stay and Play programme.

Support for children who are attending Nursery School during a local or national lockdown

Due to the practical nature of learning for young children It is unlikely that Nursery staff will ever teach on line however if staff were to need to contact children on line then the following will be considered::-

- No 1-1 discussions – group learning only.
- Where possible any on line support (eg a story session) would be pre-recorded, will take place in an appropriate room and staff will ensure that they are wearing appropriate attire.
- Practical fun ideas will be posted to parents daily via Tapestry to guide and support them in working with their child at home. Parents are also encouraged to add to their child's online portfolio by sending in photos / observations of their children engaging in activities at home. These are all sent in via Tapestry and stored in the online journal, and their child's folder, only.
- Staff will only use online platforms that have been agreed with the Head.
- Staff should ensure that the Head / Assistant Head are aware of the on line support being given, along with the date and time that it is be shared

Monitoring and reporting

a). The school network provides a level of filtering and monitoring that supports safeguarding.
b). The impact of the e-safety policy and practice is monitored through the review / audit of e-safety incident logs (appendix 5) , behaviour / bullying logs, surveys of staff, students /pupils, parents / carers
c). The records are reviewed / audited and reported to:

- the school's senior leaders
- Governors
- Halton Local Authority (where necessary)
- Halton Safeguarding Children Board

d). The school action plan indicates any planned action based on the above.

Appendices

Appendix 1 Acceptable Use Policy for any adult working with learners

Staff (and Volunteer) 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 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/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 *children's* 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 children receive opportunities to gain from the use of digital technology. I will, where possible, educate the children 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 *Federation* 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, iPad/ tablet, email, online learning journal 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 *Federation* 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/Facebook) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies ie using the Federation sites to promote the work of the school. The use of school equipment to view personal social networking sites is not permitted
- I will only communicate with children and parents/carers using official school systems. Any such communication will be professional in tone and manner. Staff should not use their personal email addresses/mobile phones/social networking sites for such communications.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

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

- When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using *Federation* equipment. I will ensure that mobile phones are stored out of the Nursery environment / locked away during Nursery hours. If they are linked to Federation wifi I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will only use personal email addresses on the school/academy ICT systems for work related purposes.
- 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/academy policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist 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.
- I will not disable or cause any damage to school/academy equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Federation Data Protection Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal 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 Federation 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 *Federation*:

- I understand that this acceptable use policy applies not only to my work and use of Federation digital technology equipment in school, but also applies to my use of Federation systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the Federation
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and/or the Local Authority 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/Volunteer Name: .....

Signed: .....

Date: .....

AUP Guidance notes for schools and governors

The policy aims to ensure that any communications technology (including computers, mobile devices and mobile phones etc.) is used to supporting learning without creating unnecessary risk to users.

The governors will ensure that:

- learners are encouraged to enjoy the safe use of digital technology to enrich their learning
- learners are made aware of risks and processes for safe digital use
- all adults and learners have received the appropriate acceptable use policies and any required training
- the school has appointed an e-Safety Coordinator and a named governor takes responsibility for e-Safety
- an e-Safety Policy has been written by the school
- the e-Safety Policy and its implementation will be reviewed annually
- the school internet access is designed for educational use and will include appropriate filtering and monitoring
- copyright law is not breached
- learners are taught to evaluate digital materials appropriately
- parents are aware of the acceptable use policy
- parents will be informed that all technology usage may be subject to monitoring, including URL's and text
- the school will take all reasonable precautions to ensure that users access only appropriate material
- the school will audit use of technology to establish if the e-safety policy is adequate and appropriately implemented
- methods to identify, assess and minimise risks will be reviewed annually
- complaints of internet misuse will be dealt with by a senior member of staff

Appendix 2 – Parent letter – internet/e-mail use

Aspiring Foundations Federated Nursery Schools

Parent / carer name:……..
Child's name: …….

As the parent or legal guardian of the above pupil(s), I grant permission for my child to have access to use the Internet, and other ICT facilities at school.

I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using a filtered internet service, employing appropriate teaching practice and teaching e-safety skills to children where appropriate.

I will support the school by promoting safe use of the Internet and digital technology at home.

I am aware that the school permits parents/carers to take photographs and videos of their own children in school events / on school visits and that the school requests that photos/videos are not shared on any social networking site such as Facebook if the photos/videos contain images of other children. I will support the school's approach to e-Safety and will not upload or add any pictures, video or text that could upset, offend or threaten the safety of any member of the school community

Parent / Guardians' signature:…….

Your name (in block capitals): …….

Date:…….

Appendix 3 – School audit

Audit

The self-audit in should be completed by the member of the Management Team responsible for the e-safety policy.

Is there a school e-safety Policy that complies with Halton guidance? Yes

Date of latest update (at least annual): Sept 21

The Leadership team member responsible for e-safety is: Amanda Brown

The governor responsible for e-Safety is: Claire Lomax

The designated member of staff for child protection is: Amanda Brown

The e-Safety Coordinator is: Amanda Brown

The e-Safety Policy was approved by the Governors on Nov 21

The policy is available for staff at: School website and policy file

The policy is available for parents/carers at: School website

Date of E-safety training for staff: WR- 25/11/19 Dit – 26/11/19 WR; Feb 21 10 minute CPD online safety; plus INSET safeguarding annual training1st /3rd Sept 21

Date of Prevent training: 17/11/2020; Amanda Brown Prevent Referrals Online 17/2/21

Appendix 4 – Photo/video consent
School Name:
Name of child:

During the year the staff may intend to take photographs of your child for promotional purposes. These images may appear in our printed publications, on video, on our website, or on all three. They may also be used by the local newspapers.
To comply with the Data Protection Act 1998, we need your permission before we take any images of your child. Please answer the questions below then sign and date the form where shown. Please bring the completed form to school. No photographs of your child will be taken until we are in receipt of this consent.
Please circle your answer
1. May we use your child's image in our printed promotional publications? Yes / No
2. May we use your child's image on the school website/ facebook page? Yes / No
3. May we record your child's image on our promotional videos? Yes / No
4. May we use your child's image in the local press? Yes / No

Signature: ……..

Your name (in block capitals)…….

Date: ……

Appendix 5 Reporting Log

Reporting Log

Group: .....

Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		

Appendix 6

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
