E-Safety Policy

& Acceptable Use Policies

Author	HBC
Approved by Governing Body	November 2025
Review Date	November 2026
First Version Date	November 2024
Version	2

Aspiring Foundations Federated Nursery Schools (AFFNS)

E-SAFETY POLICY

Responsibilities

The member of school responsible for e-safety is **Liane Johnson**

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. They 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 age and role.

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.

More generally, schools have an important role to play in equipping children and young people to stay safe online, both in school and outside. Internet safety will usually be integral to a school's ICT curriculum and can also be embedded in PSHE and SRE. 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 needs 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 school's monitoring and filtering systems to be fit for purpose.

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 device to capture images and should not use their personal devices.

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. 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.

The parental letter concerning AUPs includes a paragraph concerning posting photos on social networking sites (see appendix 2)

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

Mobile phones and other devices

AFFNS recognises that staff may need to have access to mobile phones on site 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

AFFNS allows staff to bring in mobile phones for their own personal use. However, they must be kept securely at all times and are not allowed to be used in the toilets, changing rooms or in the play areas at any time. If staff fail to follow this guidance, disciplinary action will be taken in accordance to the Federation's staff code of conduct. If staff need to make an emergency call, they must do so either in the main office, Headteacher's office or the staffroom. 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 tablets available within the nursery schools and only these should be used to record visual information within the consent criteria guidelines of the local authority and the school.

Members of staff may only contact a parent/carer on school approved mobile phones.

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 office, the Headteacher's office or the staffroom. Neither are volunteers or visitors permitted to take photographs or recordings of the children without the Headteacher's permission.

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 our schools. We take a mixture of photos that reflect the school environment; sometimes this will be when children are engrossed in an activity either on their own or with 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 our schools 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 school then it should be confiscated but staff should not 'search' the phone. The incident should be passed directly to a member of the Senior Leadership Team (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.

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.

Reporting

All breaches of the e-safety policy need to be recorded on the ICT electronic reporting log which is keep securely on the secure admin drive. The details of the user, date and incident should be reported. Incidents which may lead to child protection issues need to be passed on to the Designated Safeguarding Lead (DSL) immediately – it is their responsibility to decide on appropriate action, not the class teachers or teaching assistants.

Incidents that are of a concern under the Prevent duty should be referred to the designated lead immediately who should decide on the necessary actions regarding safeguarding and the Channel Panel.

Incidents which are not child protection issues but may require intervention (e.g. cyberbullying) should be reported to the Headteacher on the same day.

Allegations involving staff should be reported to the Headteacher. If the allegation is one of abuse, then it should be handled according to the DFE document titled 'Dealing with allegations of abuse against teachers and other staff'. If necessary, the local authority's LADO should be informed.

Evidence of incidents must be preserved and retained.

The curriculum will cover how pupils should report incidents (e.g. Ceop button, trusted adult, ChildLine).

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). Staff are encouraged to undertake additional e-safety training such as CEOP training or the European Pedagogical ICT Licence (EPICT) E-Safety Certificate
f). The culture of the Federation ensures that staff support each other in sharing knowledge and good practice about e-safety
g). The Federation takes every opportunity to research and understand good practice that is taking place in other schools
h). Governors are offered the opportunity to undertake training.

Monitoring and reporting

a). The Federation 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, surveys of staff, parents / carers
c). The records are reviewed / audited and reported to:

- The Federation'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
The policy aims to ensure that any communications technology is used without creating unnecessary risk to users whilst supporting learning.

I agree that I will:

- only use, move and share personal data securely
- respect the school network security
- implement the Federation's policy on the use of technology and digital literacy including the skills of knowledge location, retrieval and evaluation, the recognition of bias, unreliability and validity of sources
- respect the copyright and intellectual property rights of others
- only use approved email accounts
- only use pupil images or work when approved by parents and in a way that will not enable individual pupils to be identified on a public facing site.
- use the ICT facilities sensibly, professionally, lawfully, consistent with my duties and with respect for pupils and colleagues.
- not use or share my personal (home) accounts/data (eg Facebook, email, ebay etc) with parents
- set strong passwords which I will not share and will change regularly (a strong password is one which uses a combination of letters, numbers and other permitted signs).
- report unsuitable content and/or ICT misuse to the Headteacher or OneTec.
- promote any supplied E safety guidance appropriately.

I know that anything I share online may be monitored.
I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

I agree that I will not:

- visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
    - inappropriate images
    - promoting discrimination of any kind
    - promoting violence or bullying
    - promoting racial or religious hatred
    - promoting illegal acts
    - breach any Local Authority/School policies, e.g. gambling
- do anything which exposes others to danger
- post any other information which may be offensive to others
- forward chain letters
- breach copyright law
- use personal digital recording equipment including cameras, phones or other devices for taking/transferring images of pupils of staff without permission
- store images or other files off site without permission from the head teacher of their delegate representative

I will ensure that any private social networking sites, blogs, etc that I create or actively contribute to, do not compromise my professional role.

I understand that data protection policy requires me to keep any information I see regarding staff or pupils which is held within the schools' management information system private, secure and

confidential. The only exceptions are when there is a safeguarding issue, or I am required by law to disclose such information to an appropriate authority.

I accept that my use of the Federation and Local Authority ICT facilities may be monitored, and the outcomes of the monitoring may be used.

***Signed* _____**

Your name (in block capitals): …….

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 Federation
- 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 Federation will take all reasonable precautions to ensure that users access only appropriate material
- the Federation will audit use of technology and 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 (Included in admission's pack)

AFFNS

Parent / guardian name:……..

Pupil name: …….

Pupil's Key Person: ……

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.

I am aware that the school permits parents/carers to take photographs and videos of their own children in school events 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 / Guardian 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 / No

Date of latest update (at least annual):

The Leadership team member responsible for e-safety is:

The governor responsible for e-Safety is: ……..

The designated member of staff for child protection is:

The e-Safety Coordinator is: ……

The e-Safety Policy was approved by the Governors

The policy is available for staff on the

The policy is available for parents/carers at

Date of E-safety training for staff ……..

Date of Prevent training …….

Appendix 4 – Photo/video consent (Included in admission's pack)
School Name:
Name of pupil:
Class:

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 2018, 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 the ceremony. 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/SLG? 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: ……..:

Version Control and Change History

Version Control	Date Released	Review Date	Amendment
2	Sept 25	Nov 26	Page 9 – 24/7 changed to OneTec