Aspiring Foundations Federated Nursery Schools

Online 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

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

- *Keeping Children Safe in Education 2020*
- *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 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. 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 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 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.

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.

The parental letter concerning AUP's 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

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.

Reporting

All breaches of the e-safety policy need to be recorded in the ICT reporting book that is kept in the general office. 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 teacher immediately – it is their responsibility to decide on appropriate action not the class teachers.

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 senior member of staff on site in 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 Allegations Against Adults Policy

Evidence of incidents must be preserved and retained.

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. 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.
- 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, 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
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 schools 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; and the use of personal mobile phones
- 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.
- only give permission to pupils to communicate online with trusted users.
- 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 pupils or 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 named e-Safety officer
- 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 or staff without permission
- store images or other files off site without permission from the head teacher or their delegated 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 school's 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 school 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 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): March ‘18

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 9th March ‘18

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 3rd Sept 18

Date of Prevent training 6/6/16; 21/7/16; Jan 17

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: …………………………………………