

**The Federation of Kintore Way Nursery School & Children's Centre & The Grove
Nursery School**
Online Safety and Digital Media & Internet access policy

It is our duty to protect all children within our care, complying with all relevant legislation.

The Internet

The Internet is now regarded as an essential resource to support teaching and learning. Computer skills are vital to accessing life-long learning and employment. It is important for children to learn to be e-safe from an early age and the Federation can play a vital part in starting this process.

The figures for internet use show over one in three children aged 3-4 year use the internet. OFCOM Media research findings indicate that 37% use the internet via a PC, laptop or netbook, 6% via a tablet computer, and 3% via a mobile phone. (OFCEM Children and Parents: Media Use and Attitudes Report, Oct 2012)

In line with our other policies that protect children from other dangers, there is a requirement to provide children with as safe an internet environment as possible and a need to begin to teach them to be aware of and respond responsibly to possible risks.

The following control measures have been put in place in order to manage internet access and minimise risks:

- Secure broadband or wireless access
- A secure, filtered, managed internet service provider and/or learning platform
- Secure email accounts
- Regularly monitored and updated virus protection
- A secure password system
- An agreed list of assigned authorised users with controlled access
- Should children, or adults discover any potentially unsafe or inappropriate material, they are to hide the content from view by minimising or tuning off the monitor (not computers)
- All users are to be responsible for reporting any concerns encountered using online technologies to the Designated Person for Safeguarding. (The Executive Headteacher)
- Staffs are not permitted to use work-related technologies for personal access to Social networking sites
- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.
- The Executive Headteacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- Cyber bullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the Federation's policy on antibullying and behaviour.

In addition to the above control measures, Staff will:

- Be professional when using e-mail from school
- Not use inappropriate or unacceptable language
- Not reveal their personal address or telephone number or those of children or staff to people without authorisation.
- Know that access should only be made via the authorised account and password, which should not be made available to any other person.
- Not participate in any activity that threatens the integrity of the school ICT systems, or that attacks or corrupts other systems.
- Will not open any attachment to any email that is not expected or been negotiated prior to its receipt. (This is how viruses spread).
- Not use the Internet for personal financial gain, gambling or political purposes.
- Ensure that copyright of materials is respected.
- Not post anonymous messages or forward chain letters under any circumstances.
- Block network access to inappropriate materials such as pornographic, racist or offensive materials.
- Children will never use the Internet without the presence of a responsible adult

In order to support online safety in the home, the Federation will share materials with parents/carers.

Filtering and Monitoring

ICT misuse - Handling online safety complaints

- All incidents will be dealt with promptly and reported to the Senior Designated Person for Safeguarding immediately - The Executive Headteacher
- The context, intention and impact of the alleged misuse will be considered and recorded.
- Any complaint about staff misuse must be referred to the Executive Headteacher
- Complaints of a safeguarding nature must be dealt with in accordance with the Federation's safeguarding procedures.
- Discussions will be held with the relevant organisation to establish procedures for handling potentially illegal issues.
- The following incidents will be reported to the Police, Children's Social Care, Local Authority Designated Officer and Ofsted:
 - Discovery of indecent images of children
 - Behaviour considered to be 'grooming'.
 - Sending of obscene materials.

Camera and image

- General signed consent to take photographs or record images of children will be requested from the parents/carers on the wellbeing form.
- Individuals who do not have parental responsibility, such as child-minders, friends or other relatives will not be able to give such consent.

- The taking or making of images in sensitive areas of the early years setting, for example, toilet cubicles and changing areas are not permitted.
- No child's name or any other identifying information will appear in any caption or accompanying text alongside their photograph.
- Where group photographs of children and young people are to be planned, permission must be obtained from all parents and carers.
- In order to preserve the identity of children, no personal details, such as home telephone numbers, email or home addresses are to be disclosed in any written or verbal communications. This is to include information that will contribute to the personal profile of a child.
- There may be occasions where the press are invited to a planned event to take photographs of the children and young people who are to take part. It should be noted that the press enjoy special rights under the Data Protection Act, which permit them to publish material for journalistic purposes. In this circumstance, parental/carer consent will be sought before the press is to given any access to children.
- Parents and carers will only be permitted to make recordings or take photographs of any event for their own personal use. These are not to be uploaded on any social networking sites.
- CCTV is used at the reception to monitor security.
- Any images used will be copy protected and under no circumstances will a child's photo be published on any social networking site, such as Facebook.
- Either school's digital cameras should only be used on the relevant school premises. Cameras may only be taken off site for home visits and authorised trips.
- Memory sticks are not permitted under GDPR regulations
- All work-related documents and images should be backed up at the relevant school.
- Wherever possible staff should not remove photographs of children off site (e.g. in learning journey books) without informing a member of the SLT.

Mobile phone and Electronic Devices:

- All staff are encouraged not to use their own personal mobile phones for contacting parents and carers, except in emergency situations. E.g. unable to locate a parent's address during a home visit. In these instances, the staff members phone number is to be blocked by using 151 at the beginning of the number when dialling.
- All mobile phones are to be switched off or put on silence (not vibrate) and stored in staff's personal lockers during classroom hours. Staff may access their mobiles during break periods.
- Everyone, including parents, carers, visitors and contractors will be respectfully advised that their mobile phones are not to be used in the classrooms and playgrounds where children are present. Mobiles prohibited signs are visibly displayed to indicate the 'Mobile Free' areas.
- A designated work mobile is provided to be used as an effective communication tool, enabling text, email messages and calls to be made and received, to be taken on short trips and outings as well as serving as a back-up facility should landline facilities be unavailable or where contact needs to be made outside of operational hours.
- Personal calls are not to be made on the work mobile phone, other than in circumstances agreed.
- Smart Watches or electronic devices must not be connected to either school's Wifi and are on school/ airplane mode. Phones are kept in lockers so that the camera is disabled.

Communications Policy

- Children will be informed about the e-safety rules as appropriate to their understanding.
- All staff will be given the E-safety policy and its importance explained
- Parents' attention will be drawn to the e-safety policy in newsletters, on the web site and parents' workshops.
- Parent/Carers consent to take photographs of the children, to use images on the internet and to use images in the children's learning journey books is obtained on the well being forms.

This policy will be reviewed regularly to reflect technological developments.

The Federation will reserve the right to examine or delete any files that may be held on either computer system and to monitor any internet sites visited.

Links to other policies

Safeguarding (Child Protection)

Behaviour and Relationships Policy

Data Protection Policy

Staff Code of Conduct

Acceptable Use Policy

The Federation of Kintore Way Nursery School & Children's Centre & The Grove Nursery School

Policy Name

Federation Online Safety and Digital Media & Internet Access Policy

Adopted and signed on behalf of The Federation of Kintore Way Nursery School & Children's Centre & The Grove Nursery School by the Governing Body at the meeting on

26th March 2024

Name of Governing Body Representative

Robert Weir

Signature of Governing Body Representative



Signature of Headteacher



Date signed: 26th March 2024

Date to be reviewed: Spring 2025