

E- SAFETY POLICY



Frobel Education's Executive Board oversee policy and procedure for its educational services:



Last Reviewed: September 2026

By: Executive Board

Date of next review: September 2027

Our organisation is committed to keeping Students in its care safe and healthy and the e- safety policy operates always under the umbrella of the **Safeguarding Policy**. The same 'staying safe' outcome outlined in Every Child Matters agenda will apply equally to the 'virtual' or digital/electronic world of communication.

We recognise that the internet plays a vital role in education and can help enrich and extend learning activities, promote achievement, and raise educational standards. The use of the internet also supports the work of staff and helps maintain the organisation's management/admin system.

Aim

The purpose of the e-safety policy is to maximise the educational benefit and fulfil the obligation of providing quality internet access to Students as part of their lifelong learning experience, whilst adopting a safe culture and minimising any associated risks. Students shall be educated about the benefits and the risks of using technology and controlling their online experience.

Internet Access

- The use of internet is a part of the curriculum and an essential tool for staff and Students.
- The use of internet enhances learning opportunities.
- The internet is used and integrated into the planning to enrich and extend learning activities.
- The internet shall benefit education by allowing access to various educational resources.

Managing Internet Access

- Internet access is designed particularly for Students' use reflecting the curriculum requirements and includes filtering appropriate to the age of Students.
- Students are given clear objectives for Internet use and are taught what Internet use is acceptable and what is not.
- Students are taught how to evaluate Internet content.
- Students are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Students are taught about appropriate application of AI and risk of plagiarism.
- Students are taught to cross-check information and validate information before accepting its accuracy.
- Students are taught how to report unpleasant Internet content or if unsuitable sites are discovered.

Internet access security

- The security and capacity of the organisation's information systems is reviewed regularly.
- Virus protection is installed and updated regularly.

Managing E-mail

- Students and staff shall only use approved e-mail accounts on the organisation's system.
- Personal e-mail or messaging between staff and Students shall not take place.
- Staff shall use the organisation e-mail address if they need to communicate with Students about their organisation work.
- Personal details of themselves or others shall not be revealed in e-mail communication, or an arrangement to meet anyone without specific permission.
- On occasions an e-mail shall be authorised before sending to an external organisation just as a letter written on organisation headed notepaper would be.
- The forwarding of chain letters is not permitted.

Managing web site content

- The point of contact on the organisation web site shall be the organisation address, e-mail and telephone number.
- Staff or Students' personal information is not published.
- The CEO has overall editorial responsibility and ensure that content is accurate and appropriate.
- The organisation's ethos is reflected in our website, ensuring that information is accurate, well presented and personal security is not compromised.
- Care is taken to ensure that all information is considered from a security viewpoint including the use of photographic material.
- Photographs of Students are not used without the written consent of the Students/ parents/carers.
- Use of site photographs is carefully selected so that any Students cannot be identified, or their image misused.
- The names of Students are not used on the website, particularly in association with any photographs.
- The copyright of all material on the website will be held by the organisation.

Social networking and chat rooms

- The organisation blocks/filters access to social networking sites (*including My Space, Facebook, and Twitter*).
- Newsgroups are blocked unless a specific use is approved by the CEO.
- Students are advised never to give out personal details of any kind which may identify them or their location. I.e. Real name, address, mobile or landline phone numbers, organisation, e-mail address, names of friends, specific interests and clubs etc.
- Students and parents are advised that the use of social network spaces outside organisation brings a range of dangers for Students.
- Students are taught the importance of personal safety when using social networking sites and chat rooms.
- Students are not allowed to access public or unregulated chat rooms.
- Staff shall not exchange social networking addresses or use social networking sites, under

any circumstances, to communicate with Students.

- Should special circumstances arise where it is felt that communication of a personal nature between a member of staff and a learner is necessary, the agreement of the CEO or Deputy CEO shall always be sought first and language used shall always be appropriate and professional.
- Refer to the Social Media Policy for further clarification of the use of Social Media by the organisation.

Managing Filtering

- The organisation works in partnership with parents/carers; the Local Authority, the DCFS and the Internet Service Provider to ensure systems to protect Students and staff are reviewed and improved regularly.
- Filtering methods are selected by the organisation in consultation with its IT partner and Executive Board to ensure that they are age and curriculum appropriate.
- Regular checks by the DSL and senior staff are undertaken to ensure that the filtering methods selected are appropriate, effective and reasonable.
- The DSL and Network Manager check the browsing history every week on Sunday afternoon, to ensure only appropriate material has been accessed. The Network Manager will keep a weekly record of this check.
- All VPN addresses are blocked.
- If staff or Students discover unsuitable sites, the URL and content shall be reported to the CEO and DSL immediately.

Potential risks

Internet and electronic communications technologies derive huge educational benefits but also carry potential risks. Some of the potential risks are highlighted below:

Content

- Students shall be protected from viewing and/or downloading adult material, violence, racist/hate sites, potential grooming and extremist material.
- Students are made aware of the potential long-term effects of any inappropriate content that they upload themselves, such as photographs, too much personal information or nasty comments about others.
- Students are educated about the need to understand that anyone can publish anything they wish on the Internet, so it may be inaccurate.
- In addition, Students are educated about the need to understand about inappropriate use of Internet and respecting copyright issues.

Contact

There are people who will try their utmost to gain access to Students to do them harm. The dangers of contact with persons unknown are made clear.

Communication

- Students shall be protected and made aware of the potential dangers of digital communication (i.e. you can never be 100% sure that you know who you are communicating with!).
- Safe use/potential dangers of email use, instant messaging, chat rooms, social networking sites etc. are explored and made clear to Students.
- The dangers of using digital imaging devices such as cameras and webcams to display images should also be highlighted.

Culture

The way that some Students use the Internet can lead to depersonalisation (forgetting that in the virtual world, there is a real person) and this can lead to cyber bullying, which can become far more extreme and wide-ranging than 'face to face' bullying.

Commerce

Students shall be protected from and educated about issues surrounding commercial marketing such as spam, phishing etc.

Assessing risks

Some material available through the Internet is unsuitable for Students. The organisation takes all reasonable precautions to ensure that users access only appropriate material. However, due to the nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a organisation computer. The organisation cannot accept liability for the material accessed, or any consequences of Internet access.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Criminal Misuse Act 1990 and will be dealt with accordingly.

Access to any websites involving gambling, games or financial scams is strictly forbidden and shall be dealt with accordingly.

Introducing the e-safety policy to Students

- Students are informed that Internet use is only with adult supervision.
- Students are informed that internet use will be closely monitored, and that misuse will be dealt with appropriately.
- Students are instructed in responsible and safe use before being allowed access to the Internet.
- Lesson on e-safety and responsible Internet use, covering both organisation and home use, are taught for students studying Computer Science, or using a computer as part of their education with Frobel Education.

Staff and the e-Safety policy

- All staff are given the organisation e-Safety policy and its importance explained.
- Staff are made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential.
- Staff shall not use personal email or mobile technology to contact Students. If contact is necessary organisation telephone / email account shall be used.

- It is essential that all staff are confident about using the internet in their work and shall be given opportunities to discuss issues and develop appropriate teaching strategies.
- All new staff are given a copy of the policy during their induction.
- Staff development in safe and responsible use of the internet shall be provided as required.

Parent/Carers Support

- Parents/carers are informed of the Organisation's Internet Policy which can be accessed on the organisation website.
- Parents' attention is drawn to the Organisation E-safety Policy in newsletters.
- Any issues concerning the internet shall be handled sensitively to inform parents/carers without undue alarm.
- Parents and carers shall from time to time be provided with additional information on E- safety.
- The organisation requires all new Students or their parents to sign the parent/ learner agreement when they register with the organisation.
- Periodically workshops and/or podcasts are held to update awareness on E-safety.

Handling E-safety complaints

- Students and parents are informed of the complaint's procedure.
- They are informed of how and where to report incidents.
- Complaints of a child protection nature shall be dealt with in accordance with child protection/safeguarding procedures.
- Complaints of Internet misuse are dealt with by the CEO and Deputy CEO.
- Any complaint about staff or learner misuse shall be referred to CEO and Deputy CEO immediately.
- Parents/carers and Students work in partnership with organisation staff to resolve any issues.
- Sanctions within the organisation discipline policy include:
 - Interview by member of SLT.
 - Informing parents or carers.
 - Removal of Internet or computer access for a period.

Roles and responsibilities

The DSL and Deputy DSLs will ensure that:

- All staff and volunteers understand and are made aware of the organisation's E-Learning/Safety Policy and arrangements.
- Staff understand that misuse of the internet may lead to disciplinary action and possible dismissal.
- All staff are included in E-Safety training.
- A commitment to E-Safety is an integral part of the safer recruitment and selection process of staff and volunteers.
- ICT security is maintained.
- Staff attend appropriate training.
- Support and training for staff and volunteers on E-Safety is provided.
- The organisation's ICT systems are regularly reviewed with regard to security.
- Virus protection is regularly reviewed and updated.
- Regularly check files on the organisation's network.

The CEO and DSL will ensure that:

- There is a senior member of the organisation's leadership team who is designated to take the lead on E-Learning/Safety.
- Procedures are in place for dealing with breaches of e-safety and security and are in line with Local Authority procedures.
- All staff and volunteers have access to appropriate ICT training.

The Role of the DSL

- The DSL takes lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems in place).
- The DSL will train and support staff – on matters of safety, safeguarding and welfare (including online and digital safety); when deciding whether to make a referral by liaising with relevant agencies; and as a source of safeguarding support, advice and expertise for all staff.
- The DSL will ensure risks associated with being online are assessed and mitigated and complete associated risk assessment/s.
- The DSL will ensure that staff understand the risks associated with being online (and the additional risks faced by vulnerable Students) and know how to keep children safe while they're online at organisation and recognise the additional risks that children with SEND face online, and know how to support them to stay safe online.
- To manage their role effectively, the DSL will understand relevant data protection legislation, especially the Data Protection Act 2018 and the UK General Data Protection Regulation.