# GREENWOOD HOUSE ASSESSMENT CENTRE
# E-SAFETY POLICY

*"At Greenwood House, we provide a safe, nurturing and stimulating educational environment, where each child will establish a secure foundation in terms of learning and wellbeing, thus developing the skills and capabilities to reach his/her full potential."*

| | |
|---|---|
| Date Policy Written | February 2024 |
| Date Policy to be Reviewed | February 2025 |
| Date Presented to Governors | |
| Signed (Headteacher) | |
| Signed (Chair of Governors) | |

Greenwood House Assessment Centre is committed to providing a safe and secure online environment for our pupils aged 4-6. This E-Safety Policy outlines guidelines, procedures, and expectations to ensure the responsible and safe use of digital technologies within the school community.

At Greenwood House we value Information and Communications Technology (ICT) as a powerful learning tool. ICT covers a wide range of resources including web-based and mobile learning. Currently the internet technologies children and young people are using, both inside school and at home include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

Whilst these ICT resources can be exciting and beneficial both in and out of the context of education, all users need to be aware of the range of risks associated with the use of Internet technologies.
In Greenwood House, we understand the responsibility to educate our pupils in e-Safety issues at a level suitable to their needs. We aim to teach them appropriate behaviours to enable them to remain both safe and legal when using the internet and related technologies, both in school and at home.

## The Networks

Pupil access to the internet within school is provided by a filtered service provided by C2K, which should ensure educational use of the resources is safe and secure, protecting users and systems from abuse.

## The Internet

The Internet is an exciting resource that can be used to engage and broaden a child's horizons. It brings the world into the classroom by giving children access to a global network of educational resources. There is no doubt that the use of the Internet is an essential skill for children as they grow up in the modern world. The Internet is, however, an open communications' channel, available to all. Anyone can send messages, discuss ideas and publish materials with little

restriction. This brings young people into contact with people from all sectors of society and with a wide variety of materials some of which could be unsuitable. Key concerns are:

## Potential Contact

Children may come into contact with someone on-line who may wish to harm them. Some adults use social networks, chat rooms or e-mail to communicate with children for inappropriate reasons. Children should be taught at a level which is appropriate to them:

- That people are not always who they say they are.
- That "Stranger Danger" applies to the people they encounter through the Internet.
- That they should never give out personal details
- That they should never meet alone anyone contacted via the Internet
- That once they publish information it can be disseminated with ease and cannot be destroyed.

## Inappropriate Content

Through the Internet there are unsuitable materials in many varieties. Anyone can post material on the Internet. Some material is published for an adult audience and is unsuitable for children e.g., materials with a sexual content or gambling.
Materials may express extreme views. E.g. some use the web to publish information on weapons, crime and racism which would be restricted elsewhere.
Materials may contain misleading and inaccurate information. E.g. some use the web to promote activities which are harmful such as anorexia or bulimia.

Children should be taught at a level which is appropriate to them:

- How to respond to unsuitable materials or requests and that they should tell a teacher/adult immediately.

## Excessive Commercialism

The Internet is a powerful vehicle for advertising. In visiting websites children have easy access to advertising which is very persuasive.

Children should be taught at a level which is appropriate to them:

- Not to fill out forms with a lot of personal details.
- Not to use an adult's credit card number to order online products.

If children are to use the Internet in places other than at school e.g. – libraries, clubs and at home, they need to be educated about how to behave on-line and to discuss problems. There are no totally effective solutions to problems of Internet safety. Teachers, pupils and parents must be vigilant.

# Roles and Responsibilities

As e-Safety is an important aspect of strategic leadership within the school, the Principal and Board of Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. It is the role of the ICT Co-ordinator (C. Geoghegan) to keep abreast of current e-safety issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and Childnet. The ICT Co-ordinator (C. Geoghegan) has responsibility for leading and monitoring the implementation of e-safety throughout the school. The Principal/ICT Co-ordinator (L. Thompson/C. Geoghegan) must have an understanding of the issues at our school in relation to local and national guidelines and advice.

## E-safety Professional Development for Staff

- Staff are the first line of defence in e-Safety and therefore e-safety must be an essential part of staff induction and part of their on-going professional development.
- All staff to receive regular information and training on e-Safety issues through the co-ordinator at staff meetings.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community.
- New staff members receive information on the school's Acceptable Use of the Internet Policy as part of their induction.

## E-Safety Information for Parents

- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used on the school website.
- The school will communicate relevant e-Safety information through the school website.
- Parents should remember that it is important to promote e-Safety in the home and to monitor Internet use.
- Keep the computer in a communal area of the home.
- Be aware that children have access to the internet via gaming stations and portable technologies such as smart phones.
- Monitor on-line time and be aware of excessive hours spent on the Internet.
- Take an interest in what children are doing. Discuss with the children what they are seeing and using on the Internet.
- Advise children to take care and to use the Internet in a sensible and responsible manner.
- Discuss the fact that there are websites/social networking activities which are unsuitable.
- Discuss how children should respond to unsuitable materials or requests.
- Remind children never to give out personal information online.
- Remind children that people online may not be who they say they are.
- Be vigilant. Ensure that children do not arrange to meet someone they meet online.
- Be aware that children may be using the Internet in places other than in their own home or at school and that this internet use may not be filtered or supervised.

# Teaching and Learning

## Internet Use

- The school will plan and provide opportunities within a range of curriculum areas to teach e-Safety.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the e-Safety curriculum.
- We aim to make the pupils aware of where to seek advice or help if they experience problems when using the Internet and related technologies, i.e. parent/carer, teacher/trusted member of staff, or an organisation such as Childline/CEOP.
- The school Internet access is filtered through the C2k managed service.
- No filtering service is 100% effective; therefore, all children's use of the Internet is supervised by an adult.
- Use of the Internet is a planned teacher led activity. Children are taught to use the Internet in response to a need e.g., a question which has arisen from work in class.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

## E-Mail

- The forwarding of chain mail is not permitted.
- Children are not given individual e-mail addresses.
- Staff must only use C2k email for school business.
- Home emails should not be used for any school related business.
- Photographs should not be sent as attachments to e-mail without the permission of the Principal (L. Thompson).
- Information about individual children should not be sent by email without the permission of the principal

## Social Networking

- The school C2k system will block access to social networking sites.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. However, we accept that some pupils will still use them; they will be advised never to give out personal details of any kind, which may identify them or their location.
- Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- School staff will not add children as 'friends' if they use these sites.
- Employees who choose to make use of social networking sites/media should be advised as follows:

- That no direct references are made to school, staff or pupils.
- That they familiarise themselves with the site's 'privacy settings' in order to ensure that information is not automatically shared with a wider audience than intended. It is recommended that as a minimum all privacy settings are set to friends only, irrespective of use/purpose.
- That they do not conduct or portray themselves in a manner which may:
    - Bring the school into disrepute;
    - Lead to valid parental complaints;
    - Be deemed as derogatory towards the school and/or its employees;
    - Be derogatory towards pupils and/or parents and carers;
    - Bring into question their appropriateness to work with children and young people.
- That they do not form on-line 'friendships' or enter into communication with parents/carers and pupils as this could lead to professional relationships being compromised.
- On-line friendships and communication with former pupils should be advised against, particularly if the pupils are under the age of 18 years.

## Mobile Technologies

- The use of portable media such as memory sticks and external hard drives will be monitored closely as potential sources of computer virus and inappropriate material.
- Staff should not store pupils' personal data and photographs on memory sticks/iPads that are removed from the school premises.
- Pupils are not allowed to use personal mobile devices/phones in school.
- Staff should not use mobile phones during pupil contact time. The use of camera phones by staff or pupils is strictly prohibited, except in emergency situations where photographic evidence may be required.
- Only software identified by the ICT Leader should be in use on classroom PCs, iPads and Laptops.
- Any other software should be used only with the permission of the Principal
- Digital cameras are used throughout the school. Staff should take care not to display or store photographs of pupils whose parents have requested that no photographs are taken.
- It is recommended that staff do not store any unnecessary photographs of pupils. Photographs which are no longer required should be cleared on a regular basis and deleted at the end of the school year.

## Managing Video Conferencing

- Videoconferencing will be via the C2k network to ensure quality of service and security.
- Videoconferencing will be appropriately supervised.

## Publishing Pupils' Images and Work

- The consent form signed by parents/guardians upon entrance to Greenwood House is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue.
- Parents/carers may withdraw permission, in writing, at any time.
- Pupils' names will not be used anywhere on the School Website, particularly in association with photographs.
- Pupil's work can only be published by outside agencies with the permission of the pupil and parents.

# Policy Decisions

## Authorising Internet Use

- Access to the Internet will be supervised by staff.
- Passwords for the use of internet on iPads must be requested from the ICT co-ordinator (C. Geoghegan).
- All staff must read and adhere to the Acceptable Use Policy and sign the Use of ICT Agreement before using any school ICT resource.

## Password Security

- Adult users are provided with an individual login username and password, which they are encouraged to change periodically. Login details should not be shared with pupils.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school network, MIS systems.
- If pupils are working under the teacher c2k username, care should be taken that there is no access to pupil data.

## Handling E-Safety Complaints

- Complaints of Internet misuse will be dealt with by a member of the Senior Leadership Team (L. Thompson, H. McIntyre, A. Stevenson & C. Geoghegan).
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Any complaint about staff misuse must be referred to the Principal (L. Thompson).

## Monitoring and Reviewing

This policy is implemented on a day-to-day basis by all school staff and is monitored by the ICT Co-ordinator (C Geoghegan).

This policy is the Governors' responsibility, and they will review its effectiveness annually. They will do this during reviews conducted between the ICT Co-ordinator (C. Geoghegan) and Designated Child Protection Co-ordinator (H.McIntyre).

# Communicating the Policy

## Staff and the E-Safety Policy

- All staff will be given the School e-Safety Policy and its importance explained.
- Any information downloaded must be respectful of copyright, property rights and privacy.
- Staff should be aware that Internet traffic could be monitored and traced to the individual user. Discretion and professional conduct is essential.
- A laptop/iPad issued to a member of staff remains the property of the school. Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to Internet access, data protection and use of software/Apps, both in and out of school.

## Parents and the E-Safety Policy

- The e-safety policy will be available on the school website and a paper copy will be available on request.

## Writing and Reviewing the E-Safety Policy

This policy is supported by the school's Acceptable Use of the Internet Policy, ICT policy and Child Protection policy. It is the responsibility of the school, staff, governors and parents. It has been agreed by the Senior Leadership Team, Staff and approved by the Governing Body.

The rapidly changing nature of the internet and new technologies means that e-Safety is an ever growing and changing area of interest and concern. Reflecting these rapid changes, the schools e-Safety policy and its implementation will be reviewed annually.

Greenwood House

**ACCEPTABLE USE OF ICT AGREEMENT**

• The use of the Internet in school must be for professional and curriculum purposes

• Always supervise the children when they are using the Internet.

• Material that is unsuitable for children should not be viewed, uploaded or downloaded.

• All web materials should be reviewed and evaluated prior to use with the children to ensure that the content is appropriate.

• Copyright and intellectual property rights must be respected.

• If you find something inappropriate as a result of a search, the site address should be reported to the ICT coordinator (C Geoghegan).

• When writing emails acceptable language must be used at all times. Do not state anything that could be interpreted as libellous.

• Staff are responsible for all emails sent and contacts made via email.

• Staff should treat outgoing and incoming email used in school as public.

•Information about individual children should not be sent by email without the permission of the principal

• Publishing on the Web must follow the guidelines set down and contained within the Acceptable Use Policy and E-Safety Policy.

• Do not respond to inappropriate emails. Inform the ICT coordinator (C Geoghegan).

• Respect the privacy of other people's work files. Only enter them if permission from the member of staff has been given.

• The use of the Internet in school for financial gain, gambling, political purposes or advertising is forbidden.

• Any incident that breaks these guidelines must be reported.

Signed: _____

Date: _____