Gladstone Primary School

E-Safety Policy

The internet is an exciting and valuable learning tool for adults and children alike. At Gladstone, we encourage the use of the internet to support and enhance children's learning and skills development. It is important to be aware of the critical part that the internet and communications technology plays in lifelong learning and the requirements of future employment. We believe that used correctly, internet access will not only raise standards, but it will support the staff's professional work and will enhance the school's management, information and business administrative systems.

We acknowledge that the increased provision of the internet in and out of school brings with it the need to ensure that learners are safe. We need to teach pupils how to evaluate internet information and to take care of their own safety and security. E-safety, which encompasses internet technologies and electronic communications, will educate pupils about the benefits and risks of using technology and provides safeguards and awareness to enable them to control their own online experience.

Aims of the e-safety policy

- To provide clear advice and guidance in order to ensure that all internet users are aware of the risks and benefits of using the internet.
- To provide suitable action should any user encounter any inappropriate conduct, contact and content online.

E-safety education

- A progressive e-safety curriculum is in place with planned lessons which are taught throughout the year by year group teachers
- At the beginning of each new year, teachers will remind children about the acceptable use agreement, explain why this is in place and a copy of the agreement signed by all children in the class can be displayed to remind children of appropriate behaviour when online
- An e-safety assembly is held at least once a year to reinforce key e-safety messages
- A staff INSET on e-safety will take place annually or more often if needed to ensure all staff, including new members of staff, are kept up to date with e-safety issues
- The governor responsible for e-safety will, where possible, attend any training or awareness sessions on e-safety, either in school or as part of the Governor training programme
- Parents and members of the wider community can access information about e-safety via the school website
- Staff will encourage children to talk and share about their internet use and not be afraid to discuss any concerns they might have with them

Internet Security

- The school internet access includes school filtering configuration provided and approved by the Local Authority which is designed to protect pupils
- The filtering will be reviewed annually and improved if necessary
- Virus protection is installed which is updated regularly
- An additional layer of restrictions is in place via our MDM system, Meraki. This focuses on iBooks, app management and Facetime
- We recognise that filtering is not foolproof and therefore encourage children to share with staff any distressing or disturbing material they may find
- Staff and children are to report any offensive email or unsuitable website or material to the e-safety manager – Mrs Helen Reilly
- There is a universal password in place for staff to access school ICT systems. The Headteacher, Deputy Headteacher and school administration officers have their own passwords. Teacher iPads are protected with a password / passcode

- All users – staff and children - are provided with a username and password for Hwb by the ICT Subject Leader. Users are responsible for the security of their username and password

Authorising internet access

- Parents will be asked to notify the school in writing if they do not wish their child to use the internet in school
- All children are expected to read and sign the Acceptable Use Agreement before using the Internet and before they receive their Hwb username and password
- Parents will be expected to support their children with this and will sign to say they have done so
- The school will keep a record of all pupils who are not granted Internet access. The record will be kept up to date, for example a pupil's access may be withdrawn
- All staff must read, agree with and sign the Staff Acceptable Use Agreement before using the Internet

Use of digital and video images

Also See Internet Social Networking Policy, Social Media Policy and Child Protection / Safeguarding Policy

- When using digital and video images, staff should inform and educate children about the risks associated with the taking, use, sharing, publication and distribution of images. This is provided for via e-safety lessons and assemblies
- Staff should recognise the risks attached to publishing their own images or videos on the internet, in particular on social networking sites
- Care should be taken when taking digital or video images that children are appropriately dressed and are not participating in activities that might bring the individuals or school into disrepute
- Written permission from parents / carers will be obtained before photographs or videos of children are posted on the internet

Email

- Children may only use approved email accounts on the school system eg. Hwb
- Children must immediately tell a teacher if they receive an offensive email, this will be reported to the e-safety manager and the incident logged
- Children must not reveal details of themselves or others in e-mail communication, such as address or telephone number, or arrange to meet anyone
- Emails sent to an external organisation must be professional in tone and content, in the same way as a letter written on school headed paper. Emails should preferably be sent from the member of staff's Hwb email address or from the school email address
- The forwarding of chain letters is not permitted

Social networking and personal publishing

See also Internet Social Networking Policy and Social Media Policy

- The school will manage its own Twitter and Facebook account ensuring that all guidelines are adhered to by all staff
- The school will not allow pupils access to personal social networking sites except those of an educational network or approved Learning Platform (Hwb)

Managing emerging technologies

- Emerging technologies will be examined for educational benefit prior to implementation
- Children are discouraged from bringing mobile phones and other electronic devices to school. However the school recognises that especially older children may need to bring their phone if they are walking to and from school alone. If any electronic device is brought into school by a pupil, it must not be used on the school premises and must be handed in to the class teacher for safekeeping

Protecting personal data

See also Data Protection Policy

- Personal data will be recorded, processed transferred and made available according to the Data Protection Act 2018
- USB sticks or iPads taken off site must be password protected or have remote wipe capability
- Staff must ensure that when referring to a child via iMessage, only the child's first name is used and the surname initial
- If staff use their home computer for school work, they must ensure it is password protected

Handling of e-safety complaints

- Complaints of Internet misuse will be dealt with by the e-safety manager who will keep a log of all e-safety incidents via My Concern
- Sanctions for internet misuse may include informing parents / carers or the removal of internet access for a set period
- Any complaint of staff misuse must be referred to the Headteacher
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures

Role of the Governing Body

The Governing Body will:

- Give overall approval of the e-safety policy
- Review the effectiveness of the policy
- Appoint a governor to be responsible for e-safety, be a member of the e-safety committee and report back to the governing body on an annual basis or more often in the light of significant new developments to e-safety or if incidents have been reported.

Role of the Headteacher

The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community.

The Headteacher will:

- Ensure all school personnel, pupils and parents are aware of and comply with this policy
- Ensure the e-safety coordinator receives suitable training to enable them to carry out their e-safety roles and to train other colleagues where relevant
- Work closely with the Governing Body and the e-safety committee to create a safe ICT learning environment
- Be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff

Role of the e-safety manager

The e-safety manager will:

- Take day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies and documents
- Ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- Provide or identify training and advice for staff
- Receive reports of e-safety incidents and create a log of incidents to inform future e-safety developments
- Liaise with the Headteacher / Senior Leadership Team and e-safety governor to discuss current issues and review incident logs
- Lead the e-safety group

Role of the e-safety group

Members of the e-safety group will:

- Be involved with the production, review and monitoring of all school e-safety documents
- Map and review the e-safety curricular provision
- Monitor incident logs
- Consult all school stakeholders about e-safety provision
- Use 360 degree safe Cymru self review tool to monitor improvement actions

Role of School Personnel

All staff will:

- Have an up to date awareness of e-safety matters and this e-safety policy
- Have read, understood and signed the Staff Acceptable Use Agreement
- Ensure all digital communications with pupils, parents and carers are on a professional level
- Be aware that internet traffic can be monitored. Discretion and professional conduct is essential.
- Take all reasonable precautions to ensure that users access only appropriate material. However due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer.
- Report any suspected misuse or unsuitable internet sites to the e-safety manager to be logged and investigated
- Ensure pupils understand and follow the e-safety policy and acceptable use agreement

Role of Pupils

All pupils will:

- Be aware of this e-safety policy
- Have read, understood and signed the Pupil Acceptable Use Agreement
- Understand to report any offensive email or unsuitable website or material to their class teacher
- Be taught to be critically aware of the materials they read, validate information before accepting its accuracy, acknowledge the source of information used and respect copyright when using Internet material in their own work.
- Understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's e-safety policy covers their actions out of school, if related to their membership of the school.

Role of Parents / Carers

All parents and carers will:

- Be aware of and have the ability to access this e-safety policy
- Be encouraged to support the school in promoting good e-safety practice
- Be encouraged to discuss the Pupil Acceptable Use Agreement with their child and the importance of e-safety both in school and at home

A partnership approach will be encouraged with parents, carers and members of the wider community. This could include information regarding e-safety on our web site, newsletters, school prospectus, e-safety workshops held by the school and/or external agencies, afternoon community sessions within our Community room.

This e-safety policy has been developed by the school's e-safety committee which is made up of

- Deputy Head Teacher / E-safety manager
- ICT Co-ordinator
- Staff – including admin and support staff
- Governors – including the e-safety governor

The implementation of the e-safety policy will be monitored by the e-safety committee however all the stakeholders of the school will be responsible for the implementation of the policy.

The e-Safety governor will provide feedback to the governing body.

This policy will be reviewed and updated annually or as needed.

Date of next review – Autumn 2022