Gladstone Primary School - E-Safety Policy

Gladstone Primary School

We also acknowledge that greater access to the internet, both in and out of school, carries responsibilities. It is essential that pupils learn how to assess online information critically and to protect their own safety and security. E-safety, which covers internet technologies and digital communication, teaches pupils about the benefits and risks of online activity, equipping them with the awareness and skills needed to manage their own digital experiences safely.

- 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
- 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

- Parents and members of the wider community can access information about e-safety via the school website

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

We recognise that filtering is not fool proof and therefore encourage children to share with staff any distressing or disturbing material they may find

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 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

Social networking and personal publishing

- See also Internet Social Networking Policy and Social Media Policy
- The school will manage its own Twitter 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
- 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 or WhatsApp, only the child's first name is used and the surname initial
- If staff use their home computer for schoolwork, they must ensure it is password protected
- Sanctions for internet misuse may include informing parents / carers or the removal of internet access for a set period

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
- Work closely with the Governing Body and the e-safety committee to create a safe ICT learning environment

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

- Receive reports of e-safety incidents and create a log of incidents via My Concern to inform future e-safety developments

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

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.

- This policy will be reviewed and updated annually or as needed.
- Date of next review – Autumn 2026