# GEORGE GRENVILLE ACADEMY

# E-Safety POLICY

***Date: September 2021***

Review: September 2022

**Why do we need a Policy?**

The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using ICT. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and e-mail. Computer skills are vital to access life-long learning and employment; indeed ICT is now seen as an essential life-skill and as an academy, it is important we prepare the children for life in the 21st century.

More recently, due to Covid-19, staff and pupils have had to adapt their teaching and learning to a home-based system that relies on the safe use of ICT.

Most technologies present risks as well as benefits. Internet use for work, home, social and leisure activities is expanding in all sectors of society. This brings young people into contact with a wide variety of influences, some of which – as in life generally – may be unsuitable. It is important that Academy adopt strategies for the safe and responsible use of ICT.

***It is important that teachers, parents and carers do not confuse skillful use of new technologies with an ability to perceive and avoid risk – internet and ICT literacy is unfortunately not synonymous with internet and ICT safety. -* BECTA**

As the above points out it is important not to take for granted that children who are proficient in their use of the internet, are also able to assess risk when dealing with new technology and e-learning.
It is therefore the responsibility of the Academy to ensure a safe e-learning environment for the children and the Academy as a whole. This policy aims to set out how this shall be achieved.

**What are the risks?**
The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

• **content:** being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;

• **contact:** being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and

• **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

**Why is internet use important in Academy?**

- The purpose of internet use in Academy is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the Academy's management information and business administration systems.
- It is also an essential life skill which must be taught to the children if they are to succeed in the 21st century.

**How does the internet benefit education?**

Benefits of using the internet in education include:

- Access to world-wide educational resources including museums and art galleries;
- Inclusion in government initiatives such as the DfES ICT in Academies

- Educational and cultural exchanges between pupils world-wide;
- Cultural, vocational, social and leisure use in libraries, clubs and at home;
- Access to experts in many fields for pupils and staff;
- Staff professional development through access to national developments, educational materials and good curriculum practice;
- Communication with support services, professional associations and colleagues;
- Improved access to technical support including remote management of networks;
- Exchange of curriculum and administration data with the LA and DfES.
- Mentoring of pupils and provide peer support for them and teachers
- Ability to continue the education of pupils remotely in situations where the school cannot open.

**How does internet use enhance learning?**

- The use of internet allows children to bring the wider world into the classroom.
- It allows children to explore other people, places and cultures.
- Research using the internet is a necessary life skill and using the internet in Academies means the children not only learn this skill but are also able to become independent learners.
- It connects learners with educators when working remotely.

**Why is internet safety an important issue?**

- It is the responsibility of the Academy to ensure that children at Academy are safe and protected.
- Internet use inherently presents risks and the Academy needs to plan carefully for the implementation strategies to ensure these risks are minimised.
- It is important that the children are part of the implementation of an e-safety policy so that they can identify any risks both in Academy and at home and know to access help and support.
- All members of the Academy community need to be aware of the Academy's policy on e-safety.

**The Academy's E-Safety policy**

- Children must be supervised when using the internet
- Children must only be able to access internet sites that support their learning.
- The Academy uses the Buckinghamshire Grid for Learning and has filters placed upon the content, blocking unsuitable content.
- Pupils and staff are given regular e-safety education and training, which is taught as part of their computing lessons and also planned into the new relationships curriculum. (See Relationships Policy)
- Pupils are only given e-mail addresses / VLE passwords with the permission of parents.
- Pupils and staff must not reveal their passwords to anyone.
- Staff and pupils must report any unusual website to the e-safety manager
- Pupils can only use video conferencing software with supervision
- Internet access by pupils and staff is recorded through monitoring software
- Pupils' e-mails will be regularly read by staff.

- Pupils' VLE instant messages are regularly read by staff.
- All children and staff are aware that misuse of the internet will lead to loss of access.
- Children must not download materials without permission
- Children and staff must not change the Academy computers without permission.

**The Children's Code of Practice**
To implement this and help with the children's understanding a Children's Code of Practice has been written and sent home so that it can be a discussion point between parents and children.

✓ I will only use the Internet when supervised by a teacher or adult.
✓ I will never type my personal details into a web page.
✓ I will never give my password to anyone.
✓ I will log off when I have finished a session on the computer.
✓ I will always report unusual emails/web pages to a teacher.
✓ I will report bad language to a teacher if I accidentally access any.
✓ I know the sites I visit will be checked.
✓ I know that my emails will be read by teachers.
✓ I understand that I can access only sites and material relevant for my work in Academy.
✓ I understand that I will not be able to use the Internet if I do not use it sensibly.
✓ I know that I must not attempt to download software or music from the Internet.
✓ I know that I must not attempt to change the computers in Academy in any way.

This is also discussed in Academy as part of e-learning education sessions and displayed in classrooms.

**National Online Safety**
It is the vision of George Grenville Academy to provide constant and updated information to all stakeholders regarding e-safety to ensure it becomes part of the culture of the school. The school is a certified school as part of the National Online Safety organisation. All staff will receive annual, refresher and bitesize training via the online website, including each member of staff holding a certificate for online safety. Lesson plans and e-safety resources are also accessed from this site to be used across the whole school. Parents/carers and governors are signposted to the site or to relevant resources as and when they are needed.

**E-Safety education**
The Academy recognises the importance of ongoing e-safety education. Regular internet safety lessons are taught as part of computing and PSHE sessions (forming part of the relationships curriculum). The content of these sessions is directed by the e-safety manger and is reviewed regularly in light of new government advice and changing technology. An e-safety section is available on the Academy's website. These give advice to pupils and parents and useful links. Parents are invited to e-safety talks at least once a year. Children receive an e-safety talk annually from the local police.

**Home Learning and E-Safety**
In the event of children being asked to access their education remotely from home, the school will communicate an agreed code of conduct with the parents, children and staff. The Headteacher and E-Safety Manager will continue to monitor the government's advice for schools regarding internet safety when learning remotely - safeguarding and remote education guidance for schools.

**You Tube/Website**

The school has a YouTube Channel and all videos uploaded have education child restrictions added. The school will communicate to parents the importance of supervising the pupils whilst they access videos on YouTube and materials on the school's website, to ensure all content they come across is age appropriate.

**Live Webcams in teaching and learning – safeguarding issues to consider**

- If only one child turns up to a group meeting, this meeting will be cancelled.
- Staff and children must wear suitable clothing, as should anyone else in the household.
- Any computers used should be in appropriate areas, for example, not in bedrooms; and where possible be against a neutral background.
- The live class should be recorded and backed up on the school system, so that if any issues were to arise, the video can be reviewed. These videos will not be shared.
- No photographs or videos are to be taken and put on any social media platform.
- Live classes should be kept to a reasonable length of time, or the streaming may prevent the family 'getting on' with their day
- Language must be professional and appropriate, including any family members in the background
- School will have a risk assessment regarding the use of live webcams
- Data Controllers need to reassure themselves that any teaching/learning software and/or platforms are suitable and raise no privacy issues; or use cases against the providers terms and conditions (for example, no business use of consumer products)
- Devices must be clearly named before a member of staff will admit them into the meeting.

**Where 1:1 Sessions are needed – the following protocols will be agreed.**

- Parents to agree to the 1:1 session prior to the meeting and understand the reasons
- The session is recorded which is explained to the child and parent at the start of the session.
- A responsible adult must be present with the child and needs to make themselves known at the start of the session
- Meetings to be held in a suitable environment – see above (not in the child's bedroom)
- The meeting is private and a passcode will be issued to the parent to access it.

**The e-safety manager**

The Academy has appointed an e-safety manager. It is their responsibility to ensure that the Academy e-safety policy through management of staff and pupils.

The e-safety manager is responsible:

- Lead the creation of e-safety education
- Lead the parental awareness programme via the website and correspondence home.
- Have an awareness of the latest internet safety advice from the government and outside agencies such as Net Aware and NSPCC
- Meeting regularly with the head teacher to discuss e-safety issues and review progress.
- Review policy / technological solutions on basis of analysis of logs and emerging trends
- Update the governing body
- Liase with outside agencies

- Maintain a log of incidents

**Resources**

The school promote the following sites to support staff, parents and other stakeholders with a greater understanding of the risks and how these can be support in education.

- Be Internet Legends developed by Parent Zone and Google is a free internet safety curriculum with PSHE accredited lesson plans and teaching resources for Key Stage 2 pupils
- Education for a connected world framework from the UK Council for Internet Safety supports the development of the curriculum and is of particular relevance to RSHE education and Computing. It is designed, however, to be usable across the curriculum and beyond (covering early years through to age 18) and to be central to a whole school or college approach to safeguarding and online safety.
- PSHE association provides guidance to schools on developing their PSHE curriculum
- Teaching online safety in school is departmental guidance outlining how schools can ensure their pupils understand how to stay safe and behave online as part of existing curriculum requirements.
- Thinkuknow is the National Crime Agency/CEOPs education programme with age specific resources
- UK Safer Internet Centre developed guidance and resources that can help with the teaching of the online safety component of the Computing Curriculum.

**The E-Safety manager**

The Academy has appointed an e-safety manager. It is their responsibility to ensure that the Academy e-safety policy through management of staff and pupils.
The e-safety manager is responsible:

- Lead the creation of e-safety education
- Lead the parental awareness programme via the website and correspondence home.
- Have an awareness of the latest internet safety advice from the government and outside agencies such as Net Aware and NSPCC
- Meeting regularly with the head teacher to discuss e-safety issues and review progress.
- Review policy / technological solutions on basis of analysis of logs and emerging trends
- Update the governing body
- Liaise with outside agencies
- Maintain a log of incidents

**Governors**
The local governing body, alongside the Headteacher/E-Safety Manager will:

- consider a whole school approach to online safety
- ensure the school has appropriate filters and monitoring systems in place
- regularly review the school's effectiveness in online safety

**Dealing with incidents**

It is essential that any incidents are reported to the e-safety manager and followed up accordingly.

The monitoring of internet access throughout the Academy is the responsibility of the e-safety manager and if misuse is suspected this must be dealt with in the appropriate way. Children are aware that they will lose access to the internet if they behave inappropriately. Incidents of 'cyberbullying' are taken very seriously. Children are reminded that content can be seen and are encouraged to report any incidents.

If a member of staff or a child finds inappropriate content on a website they must report it to the e-safety manager who will then contact the network support team to have the site filtered.

The Academy has a procedure for dealing with incidents of inappropriate content:

1. Switch off the monitor immediately and ask the child to work on a different computer (assuming the access has been completely accidental)
2. Leave the monitor switched off until the room is free from children.
3. Make a note of the URL (web site address) and give it to the e-safety manager.
4. Clear the web site from the screen and restart the computer

Incidents of misuse are reported to the e-safety manager who will reflect on the event and decide of appropriate actions to be put in place.

It is the aim of this policy to make internet use safe and effective at George Grenville Academy. Our e-safety policy has been written by the Academy, building on the recommendations of Buckinghamshire LEA and government guidance.

It has been agreed by the senior management and approved by governors following discussions with the Student Council. It will be reviewed annually.