



# GRESTONE ACADEMY

PART OF THE HAMSTEAD HALL ACADEMY TRUST

*Perseverance • Respect • Independence • Diversity • Excellence*



## Grestone Academy E-Safety Policy

### PRIDE

**Perseverance, Respect, Independence, Diversity, Excellence.**

**Perseverance** in all we do, **Respect** for others and our environment,

Developing **Independence** as we grow.

Celebrating **Diversity** together,

Achieving **Excellence!**

Grestone Academy embraces the positive impact and educational benefits that can be achieved through appropriate use of the internet and associated communications technologies.

As a school we reward awareness from our staff and children against inappropriate use which can lead to risks and dangers. To that end, Grestone Academy provides a safe and secure environment to help educate future generations about how to stay safe in the wider world.

This policy affects all users of technological software and hardware (and other devices) owned and supplied by the school; or owned by the adults and young people who work and study within the school.

### **Objectives**

Staff and pupils have access to web sites worldwide offering educational resources, news and current events. There will be opportunities for discussion and exchange of information within the school community and others worldwide. Staff have the opportunity to access educational materials and good curriculum practice, to communicate with the advisory and support services, professional associations and colleagues; exchange curriculum and administration data with the Local Authority and Department for Education (DfE); receive up-to-date information and participate in government initiatives.

The internet is also used to enhance the school's management information and business administration systems.

### **Roles and Responsibilities**

The Head of School and Governors have ultimate responsibility for establishing safe practice and managing e-safety issues at our school.

All members of the school community have certain responsibilities within and outside the school environment. They should:

- Accept responsibility for their use of technology.
- Model best practice when using technology.
- Report any issues involving adults to the Head of School and any teaching & learning issues to the Assistant Heads of School.
- Report any incidents involving possible child protection issues direct to the DSL. Understand that network activity and online communications are monitored, including any personal and private communications made via the school network
- Be aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into force.

### **Using the internet to enhance learning**

Pupils will learn how to use a web browser. Older pupils will be taught to use suitable web search engines. Staff and pupils will begin to use the internet to find and evaluate information. Access to the internet will become a planned

part of the curriculum that will enrich and extend learning activities and will be integrated into the class schemes of work. As in other areas of their work, we recognise that pupils learn most effectively when they are given clear objectives for internet use.

Different ways of accessing information from the internet will be used depending upon the nature of the material being accessed and the age of the pupils:

- Access to the internet may be by teacher (or sometimes other-adult) demonstration;
- Pupils may access teacher-prepared materials, rather than the open internet;
- Pupils may be given a suitable web page or a single web site to access;
- Pupils may be provided with lists of relevant and suitable web sites which they may access;
- Pupils accessing the internet will be supervised by an adult, at all times. They will only be allowed to use the internet once they have been taught the Rules of Responsible Internet Use and the reasons for these rules. Teachers will endeavour to ensure that these rules remain uppermost in the children's minds as they monitor the children using the internet.

### **Using information from the internet**

In order to use information from the internet effectively, it is important for pupils to develop an understanding of the nature of the internet and the information available on it. In particular, they should know that most of the information on the internet is intended for an adult audience, much of the information on the internet is not properly audited/edited and most of it is copyright.

Staff will ensure that pupils are aware of the need to validate information whenever possible before accepting it as true, and understand that this is even more important when considering information from the internet (as a non-moderated medium). When copying materials from the Web, pupils will be taught to observe copyright.

Pupils will be made aware that the writer of an e-mail or the author of a web page may not be the person claimed.

### **Physical Environment and Security**

The school endeavours to provide a safe environment for the whole community and we review both physical and network security regularly and monitor who has access to the system consulting with the LA where appropriate.

### **Mobile / emerging technologies**

The school may at its discretion provide teaching staff with a laptop for educational use. All staff understand that the Acceptable Use Policies apply to this equipment at all times.

To ensure the security of the school systems, personal equipment is currently not permitted to be connected to the school network. Staff sometimes use their own USB sticks to transfer data.

Staff understand that they should use their own mobile phones sensibly and in line with school policy. During directed time phones must be set to silent / vibrate. Use in lessons is not allowed.

Pupils who bring mobile phones on site for travel to and from school purposes must hand phones in to the office at the start of the day and collect at the end of the school day.

The Educations and Inspections Act 2006 grants the Head the legal power to confiscate mobile devices where there is reasonable suspicion of misuse and the Head will exercise this right at their discretion.

Pictures / videos of pupils should not be taken on personal devices.

New technologies are evaluated and risk assessed for their educational benefits before they are introduced to the school community.

### **E-mail**

The school e-mail system is provided, filtered and monitored by Link2ICT and is governed by Birmingham City Council E-mail Use Policy.

All staff are given a school e-mail address and understand that this must be used for all professional communication. Currently, pupils are not provided with a school e-mail address.

Everyone in the school community understands that the e-mail system is monitored and should not be considered private communication.

Staff are allowed to access personal e-mail accounts on the school system outside directed time and understand that any messages sent using the school equipment should be in line with the e-mail policy. In addition, they also understand that these messages will be scanned by the monitoring software.

### **Published content**

The Head takes responsibility for content published to the school web site, but delegates general editorial responsibility to the PA to the Head of School.

Class teachers are responsible for the editorial control of work published by their students.

The school will hold the copyright for any material published on the school web site or will obtain permission from the copyright holder prior to publishing with appropriate attribution. The school does not publish any contact details for the pupils.

### **Digital Media**

We respect the privacy of the school community and will obtain written permission from staff, parents, carers or pupils before any images or video are published or distributed outside the school.

Photographs will be published in line with Becta guidance and not identify any individual pupil.

Students' full names will not be published outside the school environment.

Written permission will be obtained from parents or carers prior to pupils taking part in external video conferencing.

### **Social Networking and online communication**

The school is reviewing the use of social networking sites and online communication and currently does not allow access to these sites. Guidance is provided to the school community on how to use these sites safely and appropriately. This includes; not publishing personal information, not publishing private information relating to the school community how to report issues or inappropriate content.

Unmoderated chat sites present an unacceptable level of risk and are blocked in school. Pupils are given age appropriate advice and guidance around the use of such sites during Safer Internet Day and Anti-Bullying Week. All contact with pupils or ex-pupils is not allowed.

Communications between staff should abide by school policies and any incidences of inappropriate behaviour should be reported to the Head of School.

### **Educational Use**

School staff model appropriate use of school resources including the internet.

Where appropriate, links to specific web sites will be provided instead of open searching for information.

Students will be taught how to conduct safe searches of the internet and this information will be made available to parents and carers.

Teachers will be responsible for their own classroom management when using ICT equipment and will remind pupils of the Acceptable Use Policies before any activity.

### **E-safety training**

The school has a program of continuing professional development in place that includes whole school inset, in school support, consultancy and course attendance.

E-Safety is embedded throughout the school curriculum and visited by each year group, e.g. Safer Internet Day, Anti-Bullying Week.

Pupils are taught how to validate the accuracy of information found on the internet. Parents' information is available via the school website to provide appropriate advice and guidance.

### **Data Security / Data Protection**

Personal data will be recorded, processed, transferred and made available in line with the Data Protection Act 1998. Data is stored on the school systems and transferred in accordance with the Becta Data Security Guidelines.

### **Wider Community (including visiting teachers, students and visitors)**

Third party users of school equipment will be advised of the policies, filtering and monitoring that is in place. If needed, they will be issued with appropriate visitor accounts, usernames and passwords that will be recorded by office staff. Third party users must sign the school Acceptable Use Policy.

### **Responding to incidents**

Inappropriate use of school resources will be dealt with in line with school policies e.g. Behaviour, Anti-Bullying and Child Protection Policy.

Any suspected illegal activity will be reported directly to the Headteacher.

Third party complaints, or from parents concerning activity that occurs outside the normal school day, should be referred directly to the Headteacher.

Breaches of this policy by staff will be investigated by the Headteacher. Action will be taken under Birmingham City Council's Disciplinary Policy where a breach of professional conduct is identified. Incidents will be fully investigated and appropriate records made on personal files with the ultimate sanction of summary dismissal reserved for the most serious of cases involving gross misconduct.

Student policy breaches relating to bullying, drugs misuse, abuse and suicide must be reported to the nominated child protection representative and action taken in line with school anti-bullying and child protection policies. There may be occasions when the police must be involved.

Serious breaches of this policy by students will be treated as any other serious breach of conduct in line with school Behaviour Policy. For all serious breaches, the incident will be fully investigated, and appropriate records made on personal files with the ultimate sanction of exclusion reserved for the most serious of cases.

Minor student offences, such as being off-task visiting games or email websites will be handled by the teacher in situ by invoking the school behaviour policy.

The Education and Inspections Act 2006 grants the Head the legal power to take action against incidents affecting the school that occur outside the normal school day and this right will be exercised where it is considered appropriate. Implementation of policy. All staff and pupils are responsible for following this e-safety policy.