Greig City Academy

e-Safety Policy

This policy was approved by the Student and Community Committee of the Governing Body on 14 January 2020.

It will be reviewed in 2023 or prior to that if there are any legislative changes or school requirements that affect its provisions.

This policy is published on the Academy's website www.greigcityacademy.co.uk and is available on request to the Principal's PA, V. Oxley, in the following formats: e-mail, enlarged print version, others by arrangement.

1. Purpose

1.1 This policy sets out:

- how the Academy aims to ensure the safe use of internet and electronic communications technologies such as mobile phones and wireless connectivity – both existing and emerging technologies
- how staff will communicate to students the benefits and risks of using new technologies and media in and out of school
- the safeguards and rules that will guide all users in their online activities

1.1 The policy will operate in conjunction with the Academy's other policies including those for safeguarding and child protection, behaviour, anti-bullying, acceptable use of the internet, the curriculum and data protection.

2 Teaching and Learning

2.1 The Internet is an essential element of life in education, business and social interaction and is part of the statutory curriculum. Students use the Internet widely outside school and need to learn how to evaluate information and to take care of their own safety and security. For these reasons, the school has a duty to provide students with high-quality Internet access as part of their learning experience. The Academy will ensure that:

- Access levels to the Internet will reflect curriculum requirements and the age and ability of students.
- Clear boundaries will be set for appropriate use of the Internet and digital communications in accordance with the school's Acceptable Use Policy, and these will be discussed with staff and students.
- Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Students will be taught how to use the Internet effectively for research, including developing the skills needed to locate and retrieve information and those needed to be critically aware of the materials they read.
- Students will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

3 Managing Internet Access

3.1 Information system security

- The security of the school's information systems and users will be reviewed regularly.
- Virus protection will be updated daily.
- Personal data sent over the Internet or taken off site will be encrypted.
- Unapproved software will not be allowed in work areas or attached to emails.
- Files held on the network will be regularly backed up and checked.
- The ICT Network Manager will review system capacity regularly.
- The use of user logins and passwords will be enforced.

3.2 Email

- Students may use only approved email accounts on the school system.
- Students must immediately tell a member of staff if they receive an offensive email.
- Students will be advised that they should not reveal their personal details or those of others in any email communication.
- Staff will use only school email accounts to communicate with students and parents/carers.
- Emails sent to an external organisation should be written carefully and, when written by a student, authorised by a member of staff before sending.

3.3 Published content and the school website

- The Principal will take overall editorial responsibility and ensure that published content is accurate and appropriate.
- When a student joins the Academy, both the student and a parent/carer will be asked to sign a form stating whether they give consent, or object, to photographs being taken/recordings being made for use in the school's publications, its website and its social media sites. In accordance with the school's Data Protection Policy, students and parents will also be informed they may withdraw their consent at any time.
- Students' full names will not be published on the website in association with photographs except with their express permission and, in the case of students in Years 7-11, their parents'/carers' permission.
- Where the media, or organisations running events for student groups, request photographs and names of students for promotional or congratulatory purposes, consent specifically for that purpose will be requested from students and, where appropriate, parents.

3.4 Management of the Learning Platforms (LPs); examples include GCSEPod, MathsWatch, HegartyMaths

- SLT and staff will regularly monitor the usage of the LPs by students and staff in all areas, in particular message and communication tools and publishing facilities.
- All users will be advised about acceptable conduct and use when using the LPs.
- Only members of the current student, parent/carers, staff and governing body community will have access to the LPs.
- All users will be mindful of copyright issues and will only upload appropriate content onto the LPs.
- When staff or students leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.
- Any concerns about content on the LPs may be recorded and dealt with in the following ways:
    - The user will be asked to remove any material deemed to be inappropriate or offensive.
    - The material will be removed by the site administrator if the user does not comply.
    - Access to the LPs for the user may be suspended.
    - The user will need to discuss the issues with a member of SLT before reinstatement.
    - A student's parent/carer may be informed.
- A visitor may be invited onto the LPs by a member of the SLT. In this instance there may be an agreed focus or a limited time slot.
- Students may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.

3.5 Social networking and personal publishing

- The ICT Network Manager will control access from the school's network to social networking, blogging and messaging sites and, in consultation with other staff, will place restrictions on/allow access to sites.
- Through year group assemblies, tutor time follow-ups and in an online workshop, students are advised:
    - about the safe use of social networking and personal publishing sites when out of school.
    - about security and encouraged to set passwords that are difficult to identify, so as to deny access to unknown individuals and to block unwanted communications.
    - never to give out personal details which may identify them, their friends and family, or their location.

    - not to publish specific and detailed private thoughts especially those that may be considered threatening, hurtful or defamatory.

- Personal publishing will be taught via age appropriate sites suitable for educational purposes and moderated by the school where possible.
- Students and parents will be advised that the use of some social network spaces outside school is inappropriate for certain age groups.
- Concerns regarding students' use of social networking, social media and personal publishing sites will be raised with their parents/carers.

3.6 Filtering

- The ICT Network Manager will control all network filtering.
- If staff or students discover an unsuitable site that is not filtered they must report it to the ICT Network Manager.
- Changes to the filtering policy will be risk assessed by staff with educational and technical experience prior to any changes.
- The Senior Leadership Team will ensure regular checks are made to ensure that filtering methods are effective.

3.7 Managing emerging communication technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before any use in school is allowed.
- Students will be taught about safe and appropriate use of personal devices both on and off site in accordance with the school's Mobile Phone and Acceptable Use Policies.

3.8 **Use of mobile phones, ipads, tablets etc.**

- Mobile phones on the school premises should be switched off and out of sight from the start of the day when students arrive on site, until 3.20pm. After 3.20pm they may be used on site but outside the school buildings. Mobile phones on the school site may be confiscated at any time by a member of staff – in accordance with the school's confiscation policy – if they consider confiscation to be appropriate.
- Students' use of personal mobile devices must not bring harm to themselves or other students nor must such use bring the school into disrepute. The way any allegations or concerns about cyber-bullying, sexting, pornography viewing etc. will be investigated is outlined in 4.3 below.
- This policy on mobile phones is currently under review by SLT.

3.9 Protecting personal data

- Personal data will be recorded, processed, transferred and made available in accordance with the school's Data Protection Policy, the Data Protection Act 2018 and the GDPR 2018.

3.10 Summary of access management

Technology	**The school's approach**
The web	The ICT Network Manager maintains web filtering software.
Email	Students may use only approved email accounts on the school system.
Instant messaging	Blocked.
Blogs	Restrictions in place on some sites.
Podcasting	Blocked.
Social networking sites	Restrictions in place on some sites.
Video broadcasting sites such as YouTube	Blocked for KS3 and 4. Sixth formers have a usage quota. Filtered content.
Chat rooms	Blocked.
Gaming sites	Blocked.
Music download sites	Blocked for most KS3/4 use. Sites made available for use in certain classes – e.g. music and media.
Wikis	Access allowed to age-appropriate sites.
Mobiles phones	Student use not allowed in school.

4. Policy Decisions

4.1 Authorisation of Internet access

- The school will maintain a list of all staff and students who are given access to the school's electronic communications.
- All staff must read and sign the Staff Acceptable Use Policy Agreement.
- Parents/carers will be asked to read and sign the school's Acceptable Use Policy Agreement for students and discuss it with their child.
- Students will be allowed to browse the Internet appropriately and only under the supervision of staff.
- If students use words from the 'watch' list, including racist, homophobic or sexist terms or any potentially pornographic terms in any internet search or in any document, a screen print is logged and checked by the ICT Network Manager, who forwards the details to the Vice Principal (Pastoral) and/or a Head of Year. This may result in access being withdrawn.
- A record will be kept of any incident resulting in a student's access being withdrawn.

4.2 Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, because of the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable materials will never appear on a school computer.
- The Governing Body of the school cannot accept liability for the material accessed or any consequences of Internet access.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and any breaches will be reported to the Police.
- The school will audit ICT use yearly to establish if the e-safety policy is adequate and that its implementation is appropriate and effective.

4.3 Responding to incidents of concern.

- The school will take very seriously any incident of IT abuse, even if it takes place off-site, if it is of a malicious or bullying nature involving students or staff.
- Incidents of cyber-bullying sexting, pornography viewing will be dealt with in accordance with the school's anti-bullying procedures and/or safeguarding policy.
- The school's Designated Safeguarding Lead will be informed and, if there is a safeguarding concern, action may include referral to children's social care services and/or the police. If there is no such referral, the school will conduct an investigation. If an offence is found to have taken place, sanctions will be applied, regardless of the location of the offence.
- The Principal or his delegate will discuss with the police any e-safety issue that may have legal implications.

4.4 Handling formal e-safety complaints

- Complaints against staff will be dealt with by the Principal in accordance with the school's disciplinary procedures.
- Complaints of a child protection nature will be dealt with in accordance with the school's safeguarding and child protection procedures.
- All other complaints will be dealt with under the school's complaints procedure.
- All e-safety complaints will be recorded, including any actions taken.
- Students and parents will be informed of the complaints procedure.

4.5 Students off site

- Providers of work placements and alternative educational provision will be informed, and given copies, of this policy and the school's student Acceptable Use Policy Agreement and asked to abide by them. Staff monitoring such provision will monitor adherence to the policies.

4.6 Community use of the Internet

- Any community user of the school's ICT facilities will be made aware of this policy and our staff Acceptable Use policy and their agreement to abide by them will be required before use is granted.

5. Communicating the Policy

5.1 Students

- Staff across all curriculum areas will schedule into their lesson planning activities designed to show students how to use the Internet and other communication technologies appropriately and safely and will also regularly remind students of the details of the school's Acceptable Use Policy Agreement.
- Students will be informed that network and Internet use is monitored.
- Students will be advised what to do if they access material with which they are uncomfortable.

5.2 Staff

- All staff will be given copies of the e-safety policy and its importance will be explained.
- Training on this policy and all school procedures relating to e-safety will be provided.
- All staff must read and sign the Staff Acceptable Use Policy Agreement.
- Staff will be made aware that network and Internet traffic can be monitored and traced to an individual user.
- Staff who manage filtering systems and/or monitor ICT use will be supervised by the Principal and will work to clear procedures for reporting issues.

5.3 Parents and carers

- Parents' and carers' attention will be drawn to the school's e-safety policy at admission interviews and on the school website.