



The John of Gaunt School
A Community Academy

Online Safety Policy

Originator	Reviewed by	Date of Review	Approved by	Date of Approval	Next Review Date	Website
School	S&C	08/05/17	Board	22/05/17	May 2019	Yes

Contents

1.....	Vision Statement	2
2. Rationale.....		3
3. How will Internet access be authorised?		3
4. How will filtering be managed?		3
5. How will the risks be assessed?		4
6. Teaching and Learning.....		4
6.2 Why is Internet use important?		4
7. How will Internet use enhance learning?		5
8. How will pupils learn to evaluate Internet content?		5
9. Communication and Content.....		6
9.1 Website content		6
9.2 Learning Platforms.....		6
9.3 Managing e-mail.....		6
9.4 On-line communications, social networking and social media.		7
9.5 Mobile phones and personal devices		7
9.6 Video Conferencing		8
9.7 Emerging Technologies		8
9.8 Cyberbullying		8
9.9 Data Protection.....		9
10. Implementation.....		9
10.1 Introducing the Policy to Students		9
10.2 Consulting with Staff		10
10.3 Parents and Online Safety.....		10
10.4 How will complaints be handled?.....		10
11. Appendix 1 – Letter to Parents re: Students Use of Social Media		

1. Vision Statement

‘Creating an irresistible climate for achievement’

- We challenge, support and encourage every student to **achieve their potential**.
- We believe **effort** and **dedication** lead to success and we **raise aspirations**.
- We **personalise our provision** to meet the needs of individuals.
- We enable our students to flourish as **confident learners and leaders** of our community.
- We create a culture where all stakeholders **feel valued, supported and proud**.
- We **work collaboratively** to improve outcomes for our students and support other schools to improve.

2. Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. This school online safety policy is in place to help ensure safe and appropriate use.

This policy applies to all members of the school community (including staff, students, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school. The policy includes detailed information on access, content, mobile phone and other personal device use and cyber bullying. Responsibilities of the school, the staff, the students and parents are also included.

This policy should be read in conjunction with both the 'Staff and Volunteer Acceptable Use Policy' and the 'Student Acceptable use agreement form'.

3. How will Internet access be authorised?

Internet access for students is seen as an entitlement on the basis of educational need and an essential resource for staff. Parental permission is sought when each student starts at the school. The school's internet provider, SWGfL, proactively monitors Internet usage for illegal (attempted access of child abuse and incitement for racial hatred) websites and will notify the local police and Wiltshire Council in these instances.

- The school keep a record of all staff and pupils who are not granted Internet access. The record will be kept up-to-date; for instance if a pupil's access is withdrawn.
- Students must individually agree to abide by the Acceptable Use Policy statement

4. How will filtering be managed?

Despite careful design, filtering systems cannot be completely effective due to the speed of change of web content. Levels of access and supervision will vary according to the student's age and experience. Internet access must be appropriate for all members of the school community from youngest student to staff.

- A log of all staff with unfiltered access to the Internet is kept and is regularly reviewed.
- A designated member of staff will review the popular permitted and banned sites accessed by the school.
- The school will work in partnership with parents; Wiltshire Council, DFE and the SWGfL to ensure systems to protect students are reviewed and improved.
- If staff or students discover unsuitable sites, the URL (web address) and content must be reported to the Internet Service Provider (SWGfL) via the Computing and Business faculty Director of Learning.
- Website logs will be regularly sampled and monitored.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal will be referred to the Internet Watch.

5. How will the risks be assessed?

As the quantity and breadth of the information available through the Internet continues to grow it is not possible to guard against every undesirable situation. The school will address the issue that it is difficult to remove completely the risk that students might access unsuitable materials via the school system.

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will 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. The school does not 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.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The head teacher will ensure that the Internet policy is implemented and compliance with the policy monitored.

6. Teaching and Learning

6.2 Why is Internet use important?

The Internet is an essential resource to support teaching and learning. 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 and mobile learning. Computer skills are vital to access life-long learning and employment; indeed ICT is now seen as an essential life-skill.

- Internet use is a part of the statutory curriculum and a necessary tool for staff and students.
- The purpose of Internet use in school is to raise educational standards, to promote student achievement, well-being and to support the professional work of

staff and to enhance the school's management information and business administration systems.

- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- The Internet is an essential part of everyday life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Students use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.

7. How will Internet use enhance learning?

Benefits of using the Internet in education include:

- Access to worldwide educational resources including museums and art galleries;
- Inclusion in the National Education Network which connects all UK schools;
- Educational and cultural exchanges between pupils worldwide;
- Vocational, social and leisure use in libraries, clubs and at home;
- Access to experts in many fields for students and staff;
- Professional development for staff through access to national developments,
- Educational materials and effective curriculum practice;
- Collaboration across networks of schools, support services and professional associations;
- Improved access to technical support including remote management of networks and automatic system updates;
- Access to learning wherever and whenever convenient.

8. How will students learn to evaluate Internet content?

Information received via the web, e-mail or text message requires good information-handling and digital literacy skills. In particular it may be difficult to determine origin and accuracy, as the contextual clues may be missing or difficult to read. A whole curriculum approach may be required.

Ideally inappropriate material would not be visible to students using the web but this is not easy to achieve and cannot be guaranteed. Students should be taught what to do if they experience material that they find distasteful, uncomfortable or threatening.

- Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Students will use age-appropriate tools to research Internet content.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.
- If staff or students discover unsuitable sites, the URL (address) and content must be reported to the South West Grid for Learning
- Schools should ensure that the use of Internet derived materials by staff and by students complies with copyright law.

- Students will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

9. Communication and Content

9.1 Website content

- The point of contact on the school web site is the school address, school e-mail and telephone number. Staff or students' personal information will not be published.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website. Photographs will be selected carefully and will not enable individual pupils to be clearly identified.
- Students' full names will not be used anywhere on the website, particularly in association with photographs.
- The nature of all items uploaded will not include content that allows the students to be identified.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

9.2 Learning Platforms

An effective learning platform or learning environment can offer schools a wide range of benefits to teachers, students and parents, as well as support for management and administration.

- The school's senior leadership team and staff will regularly monitor the usage of the learning platform by students and staff in all areas, in particular message and communication tools and publishing facilities.
- Students/staff will be advised about acceptable conduct and use when using the learning platform.
- Only members of the current student, parent/carers and staff community will have access to the learning platform.
- All users will be mindful of copyright issues and will only upload appropriate content onto the learning platform.
- When staff, students etc leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.

9.3 Managing e-mail

E-mail is an essential means of communication for both staff and students. Directed e-mail use can bring significant educational benefits and interesting projects between schools. However, the use of e-mail requires appropriate safety measures.

- Students may only use approved e-mail accounts on the school system.
- Students must immediately tell a responsible adult if they receive offensive e-mail.
- Staff will use official school provided email accounts

- Students should use email in an acceptable way. Sending images without consent, messages that cause distress and harassment to others are considered significant breaches of school conduct and will be dealt with accordingly.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

9.4 On-line communications, social networking and social media.

On-line communications, social networking and social media services are filtered in school by the SWGfL but are likely to be accessible from home.

- Students will be taught how to keep personal information safe when using online services. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Students must not reveal personal details of themselves or others in online communication, or arrange to meet anyone.
- Staff wishing to use social media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the Senior Leadership Team before using social media tools in the classroom.
- Staff official blogs or wikis should be password protected and run with approval from the Senior Leadership Team.
- Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- Students will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Students will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' under-age use of sites.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the Staff and Volunteer Acceptable Use Policy.
- In line with, 'Guidance for Safer Working Practice for Adults who Work with Children and Young People' it will not be considered appropriate for staff to engage in personal online communications with children and young people, parents or carers. Express care is also to be taken regarding the use of social networking sites.

9.5 Mobile phones and personal devices

Mobile phones and other personal devices can be used to communicate in a variety of ways with texting, camera phones and internet accesses all common features.

- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community.
- School staff may confiscate a phone or device if they believe it is being used to contravene the school's behaviour or anti bullying policy. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.
- Mobile phones and other personal devices will not be used during lessons or formal school time unless as part of an approved and directed curriculum based activity with consent from a member of staff.
- Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items.
- Mobile phones and personal devices are not permitted to be used in certain areas within the school site such as changing rooms or toilets.
- Staff are not permitted to use their own personal phones or devices for contacting students and their families within or outside of the setting in a professional capacity.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of students and will only use work-provided equipment for this purpose.

9.6 Video Conferencing

Video conferencing enables users to see and hear each other between different locations. This 'real time' interactive technology has many potential benefits in education.

- Staff must refer to the internet consent agreements prior to students taking part in video conferences.
- All video conferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- Students will ask permission from a teacher before making or answering a video conference call.
- Video conferencing will be supervised appropriately for the students' age and ability.

9.7 Emerging Technologies

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, Internet access, collaboration and multimedia tools. A risk assessment will be undertaken on each new technology for effective and safe practice in classroom use to be developed. The safest approach is to deny access until a risk assessment has been completed and safety has been established.

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

9.8 Cyberbullying

Many young people and adults find that using the internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. It is essential that students, school staff, parents and carers understand how cyberbullying is different from other forms of bullying, how it can

affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

Cyberbullying can be defined as “The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone” DCSF 2007. DfE and Childnet have produced resources and guidance that can be used to give practical advice and guidance on cyberbullying:

<http://www.digizen.org/cyberbullying>

- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school’s anti-bullying policy.
- All incidents of cyberbullying reported to the school will be recorded.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Students, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school’s Online Safety ethos.

9.9 Data Protection

The quantity and variety of data held on students, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused. The Data Protection Act 1998 gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information.

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

10. Implementation

10.1 Introducing the Policy to Students

- All users will be informed that network and Internet use will be monitored.
- An Online Safety training programme will be established across the school to raise the awareness and importance of safe and responsible internet use amongst students.
- Student instruction regarding responsible and safe use will precede Internet access.
- An Online Safety module will be included in the ICT programmes covering both safe school and home use.
- Online Safety rules or copies of the student Acceptable Use Policy will be posted in all rooms with Internet access.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.

10.2 Consulting with Staff

- The Online Safety Policy will be formally provided to and discussed with all members of staff.
- Staff should be aware that Internet traffic is monitored and reported by the SWGfL and can be traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

10.3 Parents and Online Safety

- Parents' and carers' attention will be drawn to the School Online Safety Policy in newsletters, the school brochure and on the school Website.
- A partnership approach with parents will be encouraged. This could include offering parents' evenings, demonstrations, practical sessions and suggestions for safe Internet use at home.
- Regular information will be provided to parents about how to ensure they can work with the school to ensure this resource is used appropriately both within school and home.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.
- Interested parents will be referred to organisations such as PIN, Parents Online and NCH Action for Children.
- All parents will receive support information as and when available, e.g. Know It All for Parents.

10.4 How will complaints be handled?

- Responsibility for handling incidents will be delegated to a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Students and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.

Appendix 1 – Letter to Parents re: Students Use of Social Media

12 November 2017

Dear Parents and Carers,

As a school, we believe that the use of technology can bring many advantages to young people, improving their learning opportunities, giving them different ways to have fun and giving them a multitude of ways to keep in touch with each other via social media. Young people must be aware that there are laws governing when and how images can be taken and used and also how and where drones can be operated. Drones must not be brought into school. Students should also be aware that they must not use recording devices to record people who are not aware that they are being recorded.

These devices can also bring risks and we would encourage you to speak with your child about how they can best stay safe whilst using them. We know that although covered in school, this is most effective when supported at home by adults talking about what their young people are doing on-line, checking that they are safe, and acting correctly.

We expect to work in partnership with parents to address and challenge any issues that arise from the misuse of technology and social media and particularly those that arise from the misuse that happens on home purchased devices or outside of school hours. In these cases, although we are supportive, we would expect parents / carers be primarily responsible for monitoring and dealing with the consequences of the use of the technology that they have provided or that is being used outside of school time.

We will respond to any negative behaviour in school time which results from the misuse of social media or technology following the guidance in the school's Behaviour for Learning Policy. Parents will also be told of all instances where social media / technology has been used inappropriately and if it is on a personal device or out of school hours we will ask them to deal with this at home, providing consequences where they consider it necessary.

Issues where there is a safeguarding concern will be shared with the appropriate outside agencies; this may be social care and / or the police.

If a student is repeatedly using social media inappropriately during school hours we will ask that the student hand in their devices each morning to be kept in the safe and collected each evening or asked not to bring them to school. Students found misusing technology will be banned from using the school internet for a period of time.

For advice and support on setting up parental controls, adjusting privacy settings, understanding social networks and other issues that may relate to these matters please go on-line and visit the following website:

www.nspcc.org.uk/onlinesafety or you can call the NSPCC for support on 0808 800 5002

If you have any further questions, please contact Helen Kerr, Assistant Head Teacher on Ext 203, Eugene Spiers, Assistant Head Teacher on Ext 204 or Gareth Lister Director of Learning for Computing and Business on Ext 236.

Yours Sincerely



Helen Kerr

Assistant Head Teacher