

Online Safety Policy

Gayton Junior School



Manager:	Mr E Chapman
Date Adopted:	Spring 2026
Date for review:	Spring 2027

The Online Safety Policy was produced in consultation with the Online Safety Officer, Computing Coordinator, IT Technician, Head Teacher, staff and governors.

Rationale

The Online Safety Policy is regularly reviewed and relates to other policies including those for Behaviour, Anti Bullying, Rules for Responsible Internet Use.

The statutory curriculum expects pupils to learn how to locate, retrieve and exchange information using computers. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and e-mail. Most technologies present risks as well as benefits. Internet use must be assessed and strategies used to minimise these risks.

Internet use is expanding; this brings young people into contact with a wide variety of information, some of which could be unsuitable. It is important that schools and parents adopt suitable strategies for the responsible and safe use of the Internet. In line with school policies that protect pupils from other dangers, there is a requirement to provide pupils with as safe an Internet environment as possible and a need to teach them to be aware of and respond responsibly to the risks.

Schools need to protect themselves from possible legal challenge. Schools can protect themselves by making it clear to pupils and others that the use of school equipment to access all inappropriate material is “unauthorised”.

Core Principles of Internet Safety

Guided Educational Use

Internet use should be planned, task-orientated and educational within a regulated and managed environment. Directed and successful Internet use will also reduce the opportunities for activities of dubious worth.

Risk Assessment

21st Century life presents dangers including violence, racism and exploitation from which children and young people need to be protected. At the same time, they need to learn to recognise and avoid these risks – to become “Internet Wise”. Schools need to ensure they are fully aware of the risks, perform risk assessments and implement a policy for Internet use. Pupils need to know how to cope if they come across inappropriate material. This policy informs and supports a number of other school policies, including our Education Child Protection Safeguarding Policy and our Prevent Duty Risk Assessment. All staff should read these policies in conjunction with this policy. This is particularly important with regard to the Prevent strategy, as a large portion of cases of radicalisation happen through the online medium. Staff must be vigilant when dealing with such matters and ensure that they observe the procedure for

reporting such concerns in line with that laid out in the Education Child Protection Safeguarding Policy and our Prevent Duty Risk Assessment.

A recent development in the issues faced with internet use is that of 'cyber bullying' and other forms of web-based harassment. It is incumbent on the school to inform the children on how to deal with such issues in an appropriate manner as well as educating the children in legal realities related to online activity. This is reflected in our Anti-Bullying Policy.

Responsibility

Internet safety depends on staff, schools, governors, advisers, parents and, where appropriate, the pupils themselves taking responsibility for the use of Internet and associated communication technologies. The balance between education for responsible use, regulation and technical solutions must be judged carefully.

Governors should ensure that online safety is a running and interrelated theme while devising and implementing their whole-school approach to safeguarding and related policies and procedures.

Governors will be responsible for:

- Annually reviewing the school's online safety review
- Ensuring relevant school policies are adhered to
- Monitoring any filtering and monitoring breaches via the termly Headteacher's reports
- Providing a Link Governor for Online Safety Group
- Supporting the school to devise a Cyber Security Plan
- Ensure they are up to date with their own online safety training
- Being familiar with KCSIE guidance and other relevant legislation around online safety
- Reviewing the annual online safety risk assessment

Governors might use the UKCIS guidance 'Online safety in schools and colleges: Questions from the governing board' to support them in this.

Why is Internet use important?

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance Gayton's management information and business administration systems.

Benefits of using the Internet in education include:

- Access to the World-Wide Web
- Educational and cultural exchanges between pupils world-wide
- **Staff professional development – regular updates part of annual cycle**
- Communication with support services, professional associations and colleagues
- Improved access to technical support
- Providing pupils and parents/carers with a platform to access relevant school information
- Enabling web-based learning that is directly linked to the school's curriculum.

How will Internet use enhance learning?

Gayton's Internet access has been designed expressly for pupil use and includes filtering appropriate to the age of our pupils. Our pupils are taught what is acceptable and what is not acceptable and are given clear objectives for Internet use and research. Internet access is planned to enrich and extend learning activities, with staff guiding on-line activities.

How will pupils learn to evaluate Internet content?

Pupils are taught research techniques including the use of subject catalogues and search engines. They are encouraged to question the validity, currency and origins of information – key information handling skills. They also use alternative sources of information for comparison purposes.

Microsoft Teams usage and moderation

The school uses Microsoft Teams as a way of distributing learning electronically and providing a nexus between learning at school and home. All class teachers have access to their own class's Microsoft Teams page and are able to moderate content on that page. Senior staff have access to all Microsoft Teams pages in order to provide managerial oversight.

Children able to communicate with their teachers on issues regarding school on Teams. Children are taught what constitutes appropriate communication. Parents are informed that teachers are under no obligation to use Microsoft Teams out of school hours and that therefore they and their children are responsible for content posted. Content will be moderated by school staff in school hours. The removal of children's ability to communicate via Teams is at the absolute discretion of the school staff.

The use of Artificial Intelligence (AI) systems in School

As Generative Artificial Intelligence (gen AI) continues to advance and influence the world we live in, its role in education is also evolving. There are currently 3 key dimensions of AI use in schools: learner

support, teacher support and school operations; ensuring all use is safe, ethical and responsible is essential.

We realise that there are risks involved in the use of Gen AI services, but that these can be mitigated through our existing policies, **including our Artificial Intelligence Policy (2025)**, and procedures, amending these as necessary to address the risks. We will educate staff and learners about safe and ethical use of AI, preparing them for a future in which these technologies are likely to play an increasing role.

The school acknowledges the potential benefits of the use of AI in an educational context - including enhancing learning and teaching, improving outcomes, improving administrative processes, reducing workload and preparing staff and learners for a future in which AI technology will be an integral part. Staff are encouraged to use AI based tools to support their work where appropriate, within the frameworks provided below and are required to be professionally responsible and accountable for this area of their work.

- We will comply with all relevant legislation and guidance, with reference to guidance contained in Keeping Children Safe in Education and UK GDPR.
- We will provide relevant training for staff and governors in the advantages, use of and potential risks of AI.
- We will support staff in identifying training and development needs to enable relevant opportunities.
- We will seek to embed learning about AI as appropriate in our curriculum offer, including supporting learners to understand how gen AI works, its potential benefits, risks, and ethical and social impacts.
- **We will ensure filtering and monitoring systems are updated to support the appropriate use of gen AI in school.**

The school recognises the importance of equipping learners with the knowledge, skills and strategies to engage responsibly with AI tools. As set out in the staff acceptable use agreement **and the AI policy**, staff will be supported to use AI tools responsibly, ensuring the protection of both personal and sensitive data. Staff should only input anonymised data to avoid the exposure of personally identifiable or sensitive information. Staff should always use school-provided AI accounts for work purposes. These accounts are configured to comply with organisational security and oversight requirements, reducing the risk of data breaches.

Digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and learners instant use of images that they have recorded themselves or downloaded

from the internet. However, staff, parents/carers and learners need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- when using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images.
- staff/volunteers must be aware of those learners whose images must not be taken/published. Those images should only be taken on school devices. The personal devices of staff should not be used for such purposes
- in accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other learners in the digital/video images
- staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images
- care should be taken when sharing digital/video images that learners are appropriately dressed
- learners must not take, use, share, publish or distribute images of others without their permission
- photographs published on the website, or elsewhere that include learners will be selected carefully (only pupils with prior permission) and will comply with Online Safety Policy
- learners' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- written permission from parents or carers will be obtained before photographs of learners are taken for use in school or published on the school website/social media. Permission is not required for images taken solely for internal purposes
- parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy
- images will be securely stored in line with the school retention policy
- learners' work can only be published with the permission of the learner and parents/carers.

How will e-mail be managed?

E-mail can be an essential means of communication. Staff email is provided and secured through Microsoft Office 365. All email addresses are associated with Derby City Council and can be monitored by the LA and appropriate school staff. Some members of staff have access to an encrypted email system which is used for sensitive personal data transfer regarding children (safeguarding and SEN). Pupils do not have school e-mail addresses.

Online Publishing

The school communicates with parents/carers and the wider community and promotes the school through (amend as necessary):

- Public-facing website
- Social media – Facebook
- Online newsletters – weekly, via app, website, Facebook.
- School App – ParentApp
- Microsoft Teams – Class accounts

The school website is managed/hosted by **Lead IT**. The school ensures that this policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is least risk to members of the school community, through such publications. Where learner work, images or videos are published, their identities are protected, and full names are not published. The school public online publishing provides information about online safety e.g., publishing the schools Online Safety Policy and acceptable use agreements; collating latest advice and guidance; news articles etc., creating an online safety page on the school website. The website includes an online reporting process for parents and the wider community to register issues and concerns to complement the internal reporting process. **‘Wake up Wednesday’ campaigns regarding specific risks and apps from the National College are shared weekly on the school’s social media when relevant and also, at times, electronically on the school newsletter.**

How can emerging Internet uses be managed?

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

How will social networking, social media and personal publishing be managed?

Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. 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.

- Pupils should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location.
- Staff official blogs or wikis should be password protected and run from the school website with approval from the Senior Leadership Team. Staff should be advised not to run social network spaces for pupil use on a personal basis.
- If personal publishing is to be used with pupils, then it must use age appropriate sites suitable for educational purposes. Personal information must not be published and the site should be moderated by school staff.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others by making profiles private.
- Pupils are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- All staff will ensure that their own social network profiles are secure.

How will Internet access be authorised?

Gayton allocates Internet access for staff and pupils on the basis of educational need. Internet access is available on most of the computers in school, to staff and children. Children are supervised when on the Internet and staff are aware that they should not be visiting any unsuitable sites.

How will the risks be assessed?

Gayton 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. Neither Gayton nor the LA can accept liability for the material accessed, or any consequences of Internet access. Children are asked to turn off or minimise the screen if something appropriate does appear and report this to the nearest adult.

- Methods to identify, assess and minimise risks will be reviewed regularly.
- An annual risk assessment is completed that considers and reflects the risks that our children face.

- The headteacher will ensure that the Internet policy is implemented and compliance with the policy monitored.
- An annual review of online safety will be completed by an in-school Online Safety team.

How will filtering be managed?

Gayton works in partnership with the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.

The Internet connection has separate filtering settings for staff and pupils, both can be managed and updated directly by the Media Technician.

- Senior staff and the Media Technician ensure that regular checks are made to ensure that the filtering methods selected are appropriate and effective.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the Media Technician.
- Staff should use the Filtering & Monitoring reporting tab on CPOMS which will automatically alert the Designated Safeguarding Lead and the Media Technician.

We discourage aimless surfing. Children are taught to use the Internet in response to an articulated need – e.g. a question arising from work in class. Children should be able to answer the question “Why are we using the Internet?” **The filtering and monitoring system is reviewed by the Coordinator and the Technician to ensure that filtering is appropriate and doesn't unreasonably restrict teaching about online safety and safeguarding.**

How will the internet be monitored?

All internet traffic and communication from student computers is monitored by using SENSO software that is constantly updated in response to current trends and issues identified by the ‘cloud’. Filtering and monitoring decisions are reviewed regularly and reported to governors through the termly Headteacher’s report.

How will the policy be introduced to pupils?

Many pupils know a great deal about Internet use and culture.

- Rules for Internet access are posted near all computer systems.
- Pupils are informed that Internet use is monitored (via dedicated monitoring software, accessed by the Coordinator and Technician).
- Instructions in responsible and safe use precede Internet access.

How will staff be consulted?

All staff must be aware of the terms of the 'Responsible Internet Use' statement before using any Internet resource in school.

All staff including teachers, supply staff, classroom assistants and support staff, will be provided with Gayton's E safety policy, and its importance explained.

- Staff are aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff development in safe and responsible Internet use, and on school Internet policy forms part of our induction process.

How will the Computing system security be maintained?

Gayton's Computing systems, with regard to security are reviewed regularly. Virus protection has been installed and is updated regularly.

Any new security strategies will be discussed with the LA, particularly where a wide area network connection is being planned.

- Personal data sent over the Internet will be encrypted or otherwise secured.
- Files held on Gayton's network will be regularly checked.
- The Media Technician will ensure that the system has the capacity to take increased traffic caused by Internet use.

How will complaints regarding Internet use be handled?

Responsibility for handling incidents will be delegated to a senior member of staff.

Any complaint about staff misuse will be referred to the head teacher or the Chair of Governors, should the incident involve the Head.

- As with drugs issues, there may be occasions when the police must be contacted. Early contact will be made to establish the legal position and discuss strategies.
 - Sanctions available include (behaviour management policy):
 - informing parents or carers;
 - removal of Internet or computer access for a period, which could prevent access to school work held on the system.

Online Safety and the Curriculum

Children are taught about online safety as part of our PSHE Curriculum, which is based upon the Relationships Education and Health Education Strategy for primary pupils. The updated curriculum, for implementation in September 2026, includes the following content around Online Safety:

- That people should be respectful in online interactions, and that the same principles apply to online relationships as to face-to-face relationships, including where people are anonymous. For example, the importance of avoiding putting pressure on others to share information and images online, and strategies for resisting peer pressure.
- How to critically evaluate their online relationships and sources of information, including awareness of the risks associated with people they have never met. For example, that people sometimes behave differently online, including pretending to be someone else, or pretending to be a child, and that this can lead to dangerous situations. How to recognise harmful content or harmful contact, and how to report this.
- That there is a minimum age for joining social media sites (currently 13), which protects children from inappropriate content or unsafe contact with older social media users, who may be strangers, including other children and adults.
- The importance of exercising caution about sharing any information about themselves online. Understanding the importance of privacy and location settings to protect information online.
- Online risks, including that any material provided online might be circulated, and that once a picture or words has been circulated there is no way of deleting it everywhere and no control over where it ends up.
- That the internet contains a lot of content that can be inappropriate and upsetting for children, and where to go for advice and support when they feel worried or concerned about something they have seen or engaged with online.

These objectives are covered through our Year 4 and Year 6 PSHE curriculum topic 'Being Safe' in the Autumn Term, with Year 6 building on the knowledge gained in Year 4 and both units drawing on real-time concerns picked up from online safety training.

How will parents' and carers' support be enlisted?

Parents' and carers' attention will be drawn to the Responsible Internet Use – For Children in newsletters, the Gayton brochure and on the Gayton Junior School website.

- Internet issues will be handled sensitively to inform parents and carers without undue alarm.
- A partnership approach with parents and carers will be encouraged. This could include demonstrations, practical sessions and suggestions for safe Internet use at home.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents and carers.
- **Any digital communication between staff and students / pupils or parents / carers (email and text messages) must be professional in tone and content.** These communications may only take place

on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.

Cyber Security

The DfE Cyber security standards for schools and colleges explains: “Cyber incidents and attacks have significant operational and financial impacts on schools and colleges. These incidents or attacks will often be an intentional and unauthorised attempt to access, change or damage data and digital technology. They could be made by a person, group, or organisation outside or inside the school or college and can lead to:

- safeguarding issues due to sensitive personal data being compromised
- impact on student outcomes
- a significant data breach
- significant and lasting disruption, including the risk of repeated future cyber incidents and attacks, including school or college closure
- financial loss
- reputational damage”

The ‘Cyber-security in schools: questions for governing bodies and Trustees’ guidance produced by the National Cyber Security Centre (NCSC) aims to support governing bodies’ and management committees’ understanding of their education settings’ cyber security risks. The guidance includes eight questions to facilitate the cyber security conversation between the governing body and school leaders, with the governing body taking the lead.

The school has a business continuity and incident management plan in place and is working towards meeting the DfE cyber security standards (2026).

Appendix:

- Responsible Internet Use – for children
- Consent Form



Rules for Responsible Internet Use

We use the Gayton computers and Internet connection for learning.
These rules will help us to be fair to others and keep everyone safe.

- I will not access other people's files.
- I will only use the computers for schoolwork.
- I will not bring CD ROMs, SD cards or USB sticks into school without permission.
- I will only use the Internet when a member of staff has given me permission to do so.
- I will report any unpleasant material. I understand my report would be confidential and would protect other pupils and myself.
- I understand that a teacher may check anything I have saved and will monitor any Internet sites I visit.
- I will not look for bad language or distasteful images while I'm online and I will report these to a teacher/parent if I come across them accidentally.
- I understand that if I deliberately break these rules, I could be stopped from using the Internet or computers.
- I understand that I am responsible for what I post on Microsoft Teams and need to communicate in a school-appropriate matter.

Gayton Junior School

Pupil Agreement - Responsible Internet Use

I understand Gayton rules for responsible Internet use. I will use the computer system in a responsible way and obey these rules at all times.

Please complete, sign and return to the school office.

Pupil:

Class:

Signed:

Date:

Parent and Carer Consent

I have read and understood Gayton rules for responsible Internet use and give permission for my son or daughter to access the Internet. I understand that Gayton will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that Gayton cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that Gayton is not liable for any damages arising from use of the Internet facilities.

Signed:

Date:

Please print name: