

Parkstone Grammar School



INTERNET SAFETY POLICY

DATE APPROVED	January 2026
APPROVED BY	Leadership
NEXT REVIEW	January 2027
TYPE OF POLICY	Non-statutory



INTERNET SAFETY POLICY

Parkstone Grammar School recognises the need to maintain a strategy for the effective use of the Internet as a valuable tool for learning.

AIMS OF THE POLICY

This policy aims to outline how the school can educate its students and staff to use the Internet safely. The school deploys a range of hardware and software systems to reduce online risks and has in place a set of procedures which enable staff and students to use the Internet safely and responsibly. This policy aims to outline these.

The school has the following responsibilities:

- To designate staff to be responsible for student safety and security policies related to the Internet and electronic communications, (eg e-mail).
- To ensure that all internet access is monitored.
- To provide for learners, staff and any other adults an on screen Acceptable Use Policy Agreement, before being allowed Internet access.
- To have a system of sanctions for dealing with improper use of ICT equipment and its use.
- To make parents aware of the Internet Safety policy and procedures.
- To connect to the Internet through a filtered service.
- To ensure that staff and learners are aware that their e-mail use and Internet activity is monitored.
- To follow guidelines on the use of photos and personal details on school websites.
- To follow guidelines on the use of video-conferencing and/or webcams with/by learners.
- To take reasonable precautions to prevent the misuse of mobile phones.
- To reinforce the understanding of staff and learners that material on the Internet is subject to copyright legislation.
- To include Internet Safety as part of the Wellbeing programme and assembly programme.
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Establish and follow clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism



- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

Staff of Parkstone Grammar School accept the following responsibilities:

- To implement School Policies and procedures regarding Staff and Student Internet and e-mail Acceptable Use.
- To ensure that people in their care understand and follow policies and procedures regarding Staff and Student Internet and e-mail Acceptable Use.
- Staff and Students should be aware of any potential copyright infringement.

Governors of Parkstone Grammar School accept the following responsibilities:

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will make sure all staff undergo online safety training delivered by the DSL as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates from the DSL, as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The governor who oversees online safety is Alison Holme.

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet



The Headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The Designated Safeguarding Lead (DSL)

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other pastoral staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any incidents of cyber-bullying are logged on MyConcern and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively
- **The ICT Manager**
- The ICT manager is responsible for:
 - Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
 - Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
 - Conducting a full security check and monitoring the school's ICT systems
 - Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are reported and dealt with appropriately in line with this policy



Learners in school have the following responsibilities:

- To have a responsible attitude to the use of school ICT equipment and internet / e-mail provision.
- To follow the school's policies on Acceptable Use of the Internet and e-mail.

The following activities are strictly prohibited by all members of the school community:

- Use of the Internet to harass, offend or bully any other person.
- Use of the Internet for any inappropriate or illegal purpose.
- Use of the Internet for transmission or reception of threatening or obscene material.
- Use of the Internet for transmission or receipt of illegal material from any source.
- Use of the Internet for the transmission or receipt of viruses or unlicensed software.
- Use of the Internet for any commercial purpose or profit.
- The 'Use of the Internet' also applies to the use of personal devices or other internet capable mobile communication devices in schools.

The technological landscape is constantly changing and it is important to adapt to new threats as they arise. At present the school is looking for ways of tracking, blocking or monitoring unsolicited internet access via mobile/smart phones.

Students in Years 7 to 11 are not permitted to use their mobile phones whilst in school. Years 12 and 13 students may only use their phones in sixth form designated areas or outside of buildings.

Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Be aware that their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet

Cyber-Bullying Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.



The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff.
- Ensure that the Headteacher or Deputy Headteacher is informed for permission to complete the search.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it.
- Seek the pupil's and parent's co-operation.

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the DSL / Headteacher / other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL or Headteacher immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on [screening, searching and confiscation](#) and the UK Council for Internet Safety (UKCIS) guidance



on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on [searching, screening and confiscation](#)
- UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- Our behaviour policy / searches and confiscation policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Parkstone Grammar School recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

Parkstone Grammar School will treat any use of AI to bully pupils in line with our anti-bullying/behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.



In recognition of the risks posed by rapidly evolving technology, including Artificial Intelligence (AI) tools (which may be used to create harmful content such as 'deepfakes'), all students and their parents/carers are required to accept the specific terms regarding responsible AI use. These terms cover **academic integrity, ethical conduct, and data protection (UK GDPR)**, and are formally detailed within the **Student/Parent Acceptable Use Agreement** located in the **ICT & Internet Acceptable Use Policy (Whole School)**. Adherence to this specific commitment is mandatory for all members of the school community."

This addition ensures:

- **AI Risks are Acknowledged:** It reiterates that AI misuse is understood as a safeguarding risk (e.g., through bullying/deepfakes).
- **Compliance is Centralised:** It confirms that the specific **UK GDPR** and **academic integrity** responsibilities regarding AI are codified and agreed upon via the AUP, preventing duplication across documents while maintaining legal robustness.
- **Prohibited Activities are Covered:** It reinforces that any use of AI to harass or bully is strictly prohibited and will be dealt with under the existing policies (e.g., *Anti-Bullying Policy* and *Behaviour Policy*).

SAFEGUARDING

The school recognises the need to protect users, in particular young people, from offensive and dangerous material and acknowledges the need to ensure that all users make responsible use of the Internet and this policy outlines procedures to do this.

FILTERING AND MONITORING (ONSITE)

Filtering and monitoring systems protect pupils and staff from harmful and inappropriate content online. At Parkstone we ensure all online onsite activities are monitored by Securus contracted by Parkstone to uphold the safety and monitoring of all online activities and computer usage in school. The monitoring software detects new and emerging threats alongside established sources and types of online risk and immediately alerts the Headteacher, IT Manager and Designated Safeguarding Leads of any inappropriate IT usage. These alerts are sent through by email, or in the most extreme cases by telephone for the safeguarding team to ensure the appropriate follow up.

Harmful content may be legal or illegal, and could include but are not limited to:

- Pornography
- Promotion of self-harm and/or suicide
- Misogyny
- Racism
- Fake news
- Extremist views

All staff are responsible for following safeguarding policies and procedures, reporting any problems, and monitor what's happening on screens in school.



Below is a copy of our Filtering and Monitoring Test Certificate:

Filter Test Results for Parkstone Grammar School

Tests were performed at 05/09/2023 07:52

Your Connection

Type	Organisation	Postcode
Schools	Parkstone Grammar School	BH17 7EP

IP Address	Filtering Provider	Network
CONFIDENTIAL	LightSpeed	RMIFL

Reputation: Average

Results Overview

- Child Sexual Abuse Content: ✓
- Terrorism Content: ✓
- Adult Content: ✓
- Offensive Language: ✓

Child Sexual Abuse Content

✓ **Blocked**

Description
Tests whether you are blocking websites on the IWF Child Abuse Content URL list.

Results & Recommendations
It appears that your filtering solution includes the IWF URL Filter list, blocking access to Child Sexual Abuse content online.

Terrorism Content

✓ **Blocked**

Description
Tests whether you are blocking websites on the Counter-Terrorism Internet Referral Unit list (CTIRU).

Results & Recommendations
It appears that your filtering solution includes the Counter-Terrorism Internet Referral Unit (CTIRU) URL filter list, blocking access to unlawful terrorist content online.

Adult Content

✓ **Blocked**

Description
Test whether your Internet filter blocks access to pornography websites.

Results & Recommendations
It appears that your filtering solution includes blocking for online pornography.

Offensive Language

✓ **Blocked**

Description
Accesses a page containing offensive language to test if your filtering software blocks it.

Results & Recommendations
It appears that your filtering solution includes blocking for offensive language.

Filter Test History for 217,180,28,172

Line chart showing Test, Results, Blocked, and Accessible counts from Jan 6 to Jun 7.

CORE SCHOOL VALUES

The school aims to provide a balanced curriculum which will enable all girls to develop to the full the skills and attitudes with which to cope with adult life in a rapidly changing and increasingly technological and scientific society. This policy recognises the benefits to learning from offering students the opportunity to use the Internet to support their development and learning.

LINKED POLICIES

- Internet and Email Acceptable Use Policy – Students
- Internet and Email Acceptable Use Policy – Staff
- Bring Your Own Device Policy
- Child Protection and Safeguarding Policy
- Behaviour Policy
- Complaint Procedure