



ONLINE SAFETY POLICY

Reviewing Member of Staff: Mr Ben Freeman & Mr Martin Brant

Date Updated: 18/07/2025

Date Approved By Governors: 30/10/2025

Review Date: Autumn Term 2026

Committee: Safeguarding, Risk, Finance, Estates & General Purposes

Contents

1. Aims	2
2. Legislation and guidance	2
3. Roles and responsibilities	3
4. Educating students about online safety	5
5. Educating Parents/Carers about Online Safety	6
6. Cyberbullying	6
7. Acceptable Use of the Internet in School	8
8. Students Using Mobile Devices in School	8
9. Staff Using Work Devices Outside School	9
10. How the school will respond to issues of misuse	9
11. Artificial Intelligence (AI)	9
12. Training	9
13. Monitoring arrangements	10
14. Links with other policies	10
Appendix 1: Acceptable use of the school's ICT systems and internet: agreement for students and parents/carers	11

1. Aims

Prince Henry's High School (Prince Henry's/the school) aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The four 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 (eg 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

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools on:

- [Teaching online safety in schools](#)
- [Preventing and tackling bullying](#) and [cyberbullying: advice for Headteachers and school staff](#)
- [Relationships and sex education](#)
- [Searching, screening and confiscation](#)

It also refers to the DfE's guidance on [protecting children from radicalisation](#).

It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#) and the [Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#), which has given teachers stronger powers to tackle cyberbullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so.

This policy complies with our funding agreement and articles of association.

3. Roles and responsibilities

3.1 The Governing Body

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

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

The governing body will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing body will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL).

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

The governing body will 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 those 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 Mrs L Biggs (Safeguarding, Attendance and Online Safety)

All governors will:

- Ensure that 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 (see staff ICT User Policy)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some students with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The Headteacher

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

3.3 The Designated Safeguarding Lead

Details of the school's Designated Safeguarding Lead (DSL) and Deputies are set out in our Safeguarding Children 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 body to review this policy annually 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 Network Manager to make sure the appropriate systems and processes are in place
- Working with the Headteacher, Network Manager, Chief Operating/Data Protection Officer and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's Safeguarding Children Policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyberbullying are logged 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 body
- Undertaking annual risk assessments that consider and reflect the risks children face
- 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

This list is not intended to be exhaustive.

3.4 The Network Manager

The ICT Manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure students 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 on a daily basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy

This list is not intended to be exhaustive.

3.5 All Staff and Volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, and ensuring that students follow the school's terms on acceptable use (appendix 1)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes and being aware of how to report any incidents of those systems or processes failing by informing the DSL.
- Following the correct procedures by informing the DSL and Network Manager if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyberbullying are dealt with appropriately in line with the school's Student Conduct (behaviour) Policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents/Carers

Parents/Carers are expected to:

- Notify a member of staff or the DSL of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)

Parents/Carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - [UK Safer Internet Centre](#)
- Hot topics - [Childnet International](#)
- Parent resource sheet - [Childnet International](#)

3.7 Visitors and Members of the Community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

4. Educating students about online safety

Students will be taught about online safety as part of the curriculum:

The text below is taken from the [National Curriculum computing programmes of study](#).

It is also taken from the [guidance on relationships education, relationships and sex education \(RSE\) and health education](#).

All schools have to teach:

[Relationships education and health education](#) in primary schools

[Relationships and sex education and health education](#) in secondary schools

In **Key Stage 3**, students will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Students in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of secondary school**, students will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (eg pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some students with SEND.

5. Educating Parents/Carers about Online Safety

The school will raise parents' /carers' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents/carers via the website.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with their child's Head of Year.

Concerns or queries about this policy can be raised with any member of staff or the DSL.

6. Cyberbullying

6.1 Definition

Cyberbullying 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 one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school's Student Conduct Policy.)

6.2 Preventing and Addressing Cyberbullying

To help prevent cyberbullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students 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 cyberbullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form teachers will discuss cyberbullying with their tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. This includes Personal, Social, Health and Relationships (PSHRE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyberbullying, its impact and ways to support students, as part of safeguarding training (see section 11 for more detail).

The school also provides information on cyberbullying to parents/carers via the school website so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyberbullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among students, 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.

6.3 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 students, 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 students and staff. If the search is not urgent, they will seek advice from the Headteacher or DSL
- Explain to the student why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the student'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 staff member in conjunction with the DSL / Headteacher 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 student 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 equivalent) 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 students 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

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

6.4 Artificial intelligence (AI)

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

Prince Henry's recognises that AI has many uses to help students 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.

The school will treat any use of AI to bully pupils in line with our anti-bullying and behaviour policies.

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

7. Acceptable Use of the Internet in School

All students, parents/carers, staff, volunteers and governors are expected to read and adhere to an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendix 1 of this policy (students, parents/carers) and the ICT User Policy (staff, volunteers and governors).

8. Students Using Mobile Devices in School

Any breach of the acceptable use agreement by a student may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

Students in Years 9-11

Mobile phones/electronic devices are a distraction to the learning process and are not required during school time. Any mobile phone/electronic device in plain sight will be confiscated and only returned to the appropriate parent/carer who will need to collect it from the school office. Any mobile phone or other device that is brought into school is entirely at the risk of the student. The school will not be responsible for any loss or damage to the device.

In the event of an emergency the school office is happy to pass urgent messages on to students so that the use of a mobile is **NEVER** necessary within school.

Sixth Form

Students in Years 12 and 13 are permitted to use mobile phones in the Sixth Form Centre only. In setting an example to students in the Lower School, personal devices must not be used in other parts of the school.

All Students

The filming or recording by mobile phones in school is prohibited and if the school is made aware that such activity has occurred and shared, eg via social media the school reserves the right to impose sanctions which may vary depending on the severity of the offence, including suspension or permanent exclusion even for a first offence.

Exceptions for Sixth Form Students

- Mobile phones or similar devices and headphones/ear pods have a valid use for some ICT, iMedia and Music courses as they enable students to store documents and therefore take work home with them. These devices should not be seen or used at any time other than in lessons where permission has been given. Any mobile phone or other device that is brought into school is entirely at the risk of the student. The school will not be responsible for any loss or damage to the device.
- The use of Headphones. It may be appropriate for headphones to be used with computers eg Language work, but under no circumstances should they be used simply to listen to music.

- The use of chargers by students. Students must not use their own chargers on the school site.

9. Staff Using Work Devices Outside School

The school has a separate ICT User Policy for staff of the school, which should be referred to in relation to the use of work devices outside school.

Staff are permitted to use school-owned ICT devices such as laptops, tablets, and mobile phones off-site for professional purposes, provided they do so responsibly and in line with school policies. Staff are expected to handle devices with care, ensuring they are kept secure and not left unattended in public or unsecured locations. All devices must be password-protected, and any access to personal or sensitive data must comply with the school's Data Protection Policy and UK GDPR. Staff should use secure internet connections and avoid public Wi-Fi where possible. It is important to note that all school-owned devices are subject to monitoring regardless of location; this includes internet usage, application activity, system performance, and device location. There is no expectation of privacy when using school devices, even when off-site or outside of school hours. Any misuse, breach of policy, or tampering with monitoring systems may lead to disciplinary action, and any loss, theft, or suspected compromise of a device must be reported to the ICT Support Team or Senior Leadership immediately.

10. How the school will respond to issues of misuse

Where a student misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate. Where students wilfully cause damage to ICT equipment, the school reserves the right to seek financial restitution from parents/carers.

Where a staff member misuses the school's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the Staff Disciplinary Procedures/Staff Code of Conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Artificial Intelligence (AI)

The Department for Education supports the careful and sensible use of artificial intelligence (AI) tools like ChatGPT, Copilot, and others in schools. These tools can help staff save time by supporting tasks such as planning lessons, creating resources, or giving feedback to students. However, any content produced by AI must always be checked by a member of staff to make sure it is correct and suitable. Schools should only use AI tools that follow rules about data protection and copyright and should avoid using personal accounts when accessing them. While AI has the potential to be a helpful tool in education, staff should also be aware of the risks, such as inaccurate information, bias, or students using AI inappropriately.

12. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyberbullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
 - Abusive, harassing and misogynistic messages

- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every two years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Safeguarding Children Policy.

13. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed every year by the Designated Safeguarding Lead. At every review, the policy will be shared with the governing body.

14. Links with other policies

This online safety policy is linked to our:

Safeguarding Children Policy (including Child on Child Abuse)
 Student Conduct Policy
 Staff Code of Conduct
 Staff Disciplinary Procedure
 ICT User Policy
 Social Media Policy
 Data Protection Policy and Privacy Notices
 Complaints procedure

Appendix 1: Acceptable use of the school's ICT systems and internet: agreement for students and parents/carers

Student's Agreement

I will read and follow the rules in the acceptable use agreement policy.

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my usernames and passwords safe and not share these with others
- Ensure that I use 'strong' passwords containing a mixture of letters and numbers, and that I change this on a regular (termly) basis
- Always check files brought in on removable media (eg USB sticks) with antivirus software before using them
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others that hasn't been picked up and blocked by the school network's filtering system
- Protect school IT equipment from spillages by eating and/or drinking well away from IT classrooms and IT equipment in other classrooms
- Always log off or shut down a computer when I've finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Attempt to install programs of any type on school computers
- Use websites/software in order to attempt to bypass school IT filters
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision
- Wilfully cause damage to any school ICT equipment
- Use my own chargers to charge any mobile equipment whilst in school

Sixth Form Students:

- I will not attempt to connect my personal mobile equipment (laptops, tablets, mobile devices) to the school network, but may use the internet-only guest network during lessons/private study in designated Sixth Form areas
- If I bring a personal mobile phone or other personal electronic device into school I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

If I bring a personal mobile phone or other personal electronic device into school:

- This is entirely at my own risk and I understand that the school will not be responsible for any loss or damage to the device
- Any device that is in plain sight will be confiscated and only returned to my parent/carer, who will need to collect it from the school office (students in Years 9-11)
- I will not use any device to film or record in school and understand that if the school is made aware that such activity has occurred and been shared, eg via social media, there may be serious sanctions including suspension or permanent exclusion
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

All computer use, including Email usage and internet access is monitored and recorded centrally. The school's security and network management systems record each Internet page visited by users and tracks all e-mails sent and received. Files and communications on computer storage areas and removable storage devices may also be reviewed by staff to ensure you are using the system responsibly and in line with school policies.

I agree that if I violate these provisions, access to the internet will be denied and I will be subject to disciplinary action. Where damage is wilfully caused to ICT equipment, I understand that the school reserves the right to seek financial restitution from parents/carers. Additional action may be taken by the school in line with existing policies regarding school behaviour. For serious violations, suspension or expulsion may be imposed. Where appropriate, police may be involved or other legal action taken.

Parent/carer's agreement

I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for students using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these. I understand that if my child wilfully causes damage to school ICT equipment, the school reserves the right to seek financial restitution from me.