Online Safety Policy

Date First Published	**September 2025**
Version	**1**
Last approved	**September 2025**
Review Cycle	**Annual**
Review Date	**March 2026**

An academy within:

"Learning together, to be the best we can be"

1. Policy Introduction

1.1. The Online safety policy is in place to ensure that all staff and students are supported to understand how to keep themselves safe when using the internet and associated technologies. The use of these exciting and innovative technologies in school and at home has been shown to raise educational standards and promote student achievement. However, their use can put users at risk. These risks can be categorised into three main areas:

Content: being exposed to illegal, inappropriate or harmful material

Contact: being subjected to harmful online interaction with other users

Conduct: personal online behaviour that increases the likelihood of, or causes, harm

1.2. Bents Green School is committed to ensuring that students have safe access to the internet by putting effective systems in place to stop them accessing inappropriate information. This is reinforced by a curriculum which aims to ensure all students and staff develop a safe and responsible set of behaviours which will enable them to reduce the risks of harm whilst continuing to benefit from using the Internet and new technologies.

Designated Safeguarding Lead (DSL)	Cathy Varley Emma Thomson
Online-safety lead	Cathy Varley
Online-safety / safeguarding link governor	Natalie Brownell
Online Safety Curriculum Coordinator (None Safeguarding)	Richard Cusworth Vivien Annabel
Network Manager / other technical support	Nexus IT Support
Date this policy was reviewed and by whom	January 2025 - Cathy Varley
Date of next review and by whom	January 2027 - Cathy Varley

2. Scope

2.1. This overarching Online safety policy has been developed and published to outline Bents Green School's commitment to a best practice approach in safeguarding children and young people from harm. Our aim is to have robust

processes in place to ensure the online safety of pupils, staff, volunteers and governors.

2.2. Safeguarding children is everyone's responsibility. Everyone who comes into contact with children and families has a role to play.

2.3. Our pupils' welfare is our paramount concern. The Trust, through its defined quality assurance processes, will ensure 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')

2.4. Everyone in our school is part of a community and all those directly connected - staff members, governors, parents, families and pupils - have an essential role to play in making it safe and secure.

3. Ethos

3.1. We believe that all our school should provide a caring, positive, safe and stimulating environment that promotes the social, physical and moral development of each individual child.

3.2. We recognise the importance of providing an environment within our academies that will help children feel safe and respected. We recognise the importance of enabling children to talk openly and to feel confident that they will be listened to.

3.3. We recognise that all adults within the academy - including permanent and temporary staff, volunteers and governors - have a full and active part to play in protecting our pupils from harm.

3.4. We will work with parents to build an understanding of the school's responsibilities to ensure the welfare of all children, including the need for referrals to other agencies in some situations.

4. The legal framework

4.1. This policy is based on the government'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 cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

4.2. It also refers to the DFEs guidance on protecting children from radicalisation.

4.3. 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 cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

4.4. The policy also considers the computing programmes of study within individual academies and schools.

5. Roles and responsibilities

5.1. Bents Green school is a community and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, students, families and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

5.2. The Policy Review Board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. The Trust board 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).

Trustees

5.3. All Trustees will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of ICT systems and the internet
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or academy 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 pupils with special educational needs and/or disabilities (SEND). This

is 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.

The Headteacher

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

5.5. The Headteacher will:

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Oversee the activities of the designated safeguarding lead and ensure that the DSL responsibilities listed in the section below are being followed and fully supported
- Ensure that policies and procedures are followed by all staff
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and Sheffield Safeguarding Children Partnership.
- Liaise with the designated safeguarding lead on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of students, including risk of children being radicalised
- Ensure that there is a system in place to monitor and support staff (e.g. network manager) who carry out internal technical online-safety procedures
- Ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety
- Ensure the school website meets statutory requirements

The Designated Safeguarding Lead

5.6. The Designated safeguarding lead will have lead responsibility for safeguarding and child protection including online safety.

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

- Ensure "An effective approach to online safety that empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate."
- "Liaise with staff on matters of safety and safeguarding (including online and digital safety) and when deciding whether to make a referral by liaising with relevant agencies."
- Take day-to-day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- Remind staff of safeguarding considerations as part of a review of remote learning procedures and technology, including that the same principles of online safety and behaviour apply
- Work with the headteacher, DPO and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Stay up to date with the latest trends in online safeguarding and "undertake Prevent awareness training.
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the governors/trustees.
- Ensure that online safety education is embedded across the curriculum in line with the statutory RSHE guidance (e.g. by use of the updated UKCIS framework 'Education for a Connected World – 2020 edition') and beyond, in wider school life
- Promote an awareness of and commitment to online safety throughout the school community, with a strong focus on parents, but also including hard-to-reach parents.
- Communicate regularly with SLT and the designated safeguarding and online safety governor/committee to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how filtering and monitoring work and have been functioning/helping.
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident.
- Oversee and discuss 'appropriate filtering and monitoring' with governors and ensure staff are also aware
- Be aware and make judicious use of safeguarding reports that are produced by the schools Internet Monitoring Service by working in conjunction with technical teams.
- Make key decisions on allowing access to sites and apps in schools by relaxing either temporarily or permanently some of the filtering setting within the schools filtering and monitoring system and ensure that these

decisions are logged. The DSL should prioritise keeping children safe but "be careful that 'over blocking' does not lead to unreasonable restrictions" (KCSIE 2021)

- Ensure the updated 2021 DfE guidance on Sexual Violence & Sexual Harassment Between Children in Schools & Colleges Guidance is followed throughout the school and that staff adopt a zero-tolerance, whole school approach to this, as well as to bullying.
- Facilitate training and advice for all staff, including supply teachers:
- All staff must read KCSIE Part 1 and all those working with children Annex B
- Cascade knowledge of risks and opportunities throughout the organisation
- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT team 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 safeguarding and child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying 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 board
- To support the online safety coordinator in promoting an awareness and commitment to online safety throughout the school.
- To be a point of contact in school on online safety matters (see attached protocols) – receive and regularly review online safety incident logs and be aware of the procedures to be followed should an online safety incident happen in school.
- To liaise with the local authority, the Sheffield Safeguarding Children's Board and other relevant agencies as appropriate.
- To communicate regularly with school technical staff, the Safeguarding governor, Senior Leadership Team, PSD curriculum leads.
- To maintain an up to date understanding of current online safety issues, guidance and appropriate legislation.
- To ensure that online safety is promoted to parents and carers.
- To understand the issues surrounding the sharing of personal or sensitive information.
- To understand the dangers regarding access to inappropriate online contact with adults and strangers.
- To be aware of potential or actual incidents involving grooming of young children.

- To be aware of and understand cyberbullying and the use of social media for this purpose.
- To lead any investigations of illegal / inappropriate use of technology by students in line with behaviour and discipline procedures, reporting to and consulting with wider professionals in line with the schools responses to an Incident of Concern (see page 19)
- To attend Safeguarding Refresher yearly with Sheffield City Council.

The ICT Team

5.8. The ICT team 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 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 on a weekly 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
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

All Staff and Volunteers

5.9. 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 ICT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use
- 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 cyber-bullying are dealt with appropriately in line with the school 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.

Parents\Carers

5.10. Parents\ Carers are expected to:

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

Visitors and members of the community

5.11. 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.

6. Educating and Supporting Children about Online Safety - Education and Curriculum

6.1. At Bents Green School we believe that the key to developing safe and responsible behaviours online, not only for students but for everyone within the school community, lies in a progressive and age-appropriate online safety curriculum. We know that the Internet and other technologies are embedded in our students' lives not just in school but outside as well, and we believe we have a duty to help prepare our students to safely benefit from the opportunities that the Internet brings.

6.2. Online safety education will be provided in the following ways:

- We will provide a series of specific online safety-related lessons in every year group as part of the PSD AND PSHE, computing curriculum and other lessons as appropriate.
- We will celebrate and promote online safety through a planned programme of assemblies and whole-school activities, including promoting Safer Internet Day each year.

- We will discuss, remind or raise relevant online safety messages with students routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials.
- We will remind students about their responsibilities through an Acceptable Use Policy which every student will sign and which will be displayed throughout the school.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.
- When searching the internet for information, students will be guided to use age-appropriate search engines. All use will be monitored and students will be reminded of what to do if they come across unsuitable content.
- Where appropriate students will be taught in an age / ability appropriate way about copyright in relation to online resources.
- Students will be taught about the impact of cyberbullying and know how to seek help if they are affected by any form of online bullying.
- Students will be made aware of where / how to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CEOP report abuse button

6.3. Our Pupils will be taught about online safety as part of the curriculum:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

6.4. In Key Stage 3, pupils 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

6.5. Pupils 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, pupils 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 (e.g. 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)

6.6. When educating children within our settings we keep in mind the 4 Cs of online safety. The four Cs are "content", "contact", "conduct" and "commerce".

7. Educating Parents\Carers

7.1. The school will raise parents' 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.

7.2. Online safety will also be covered during parents' evenings.

7.3. The school will let parents 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

7.4. If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

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

8. Cyber Bullying

7.1. 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.)

7.2. We help to prevent cyber-bullying by ensuring 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.

7.3. 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. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

7.4. All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

7.5. The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

7.6. 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.

7.7. 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.

8. Examining Electronic Devices

8.1. 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, the authorised staff member will:
- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff
- 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 cooperation
- 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

8.2. If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL 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.

8.3. 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 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 government'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 government'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.

9. Acceptable use of the internet in school

9.1. All pupils, parents, staff, volunteers and governors are expected to sign 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.

9.2. 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.

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

10. Staff Using Work Devices Outside School

10.1. 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

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

10.3. Work devices must be used solely for work activities.

10.4. If staff have any concerns over the security of their device, they must seek advice from the IT Team.

11. How the Trust will respond to issues of misuse

11.1. Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our behaviour policies and ICT acceptable use policy. The action taken will depend on the individual circumstances, nature, and seriousness of the specific incident, and will be proportionate.

12. Training

12.1. All new staff members will receive training, as part of their induction, on safer internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

12.2. 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).

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

12.3.1. Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse

12.3.2. 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

12.3.3. Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

12.4. 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

12.5. The DSL and deputy/deputies will undertake child protection and safeguarding refresher training, which will include online safety, annually. They will also update their knowledge and skills on the subject of online safety at regular intervals.

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

12.7. Volunteers will receive appropriate training and updates, if applicable.

12.8. More information about safeguarding training is set out in our child protection and safeguarding policy.

13. Generative AI

13.1. 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.

13.2. Bents Green 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. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

13.3. Bents Green[School] will treat any use of AI to bully pupils in line with our [anti-bullying/behaviour] policy.

13.4. 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/trust.

13.5. In line with the Trust Information Governance policy, schools should note that if personal and/or sensitive data is entered into an unauthorised generative AI tool, Nexus will treat this as a data breach and will follow the personal data breach procedure.

14. Monitoring

14.1. The DSL logs behaviour and safeguarding issues related to online safety.

14.2. DSL should take lead responsibility for auditing the effectiveness of the filtering and monitoring systems.

14.3. Staff and volunteers should oversee and monitor all online access/usage and challenge/report any misuse.

14.4. This policy will be reviewed every year by the DSL. At every review, the policy will be shared with the Policy Review Board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

The grid below shows which technologies we have agreed as a staff will be allowed in school

	Students	Staff
Personal mobiles & Smart Watches brought into school	**Year 7 – 11** Not allowed. Must be handed in on arrival to	Allowed in restricted areas of the school (offices, staffrooms and staff workrooms). They

	school. **Post-16** Allowed for some off-site activities with permission appropriate education / and supervision	**should not** be used in classrooms or any other student areas. See mobile phone policy for exceptional circumstances
Taking photographs / videos on personal equipment	**Year 7 – 11** Not allowed. **Post-16** May be allowed on some offsite visits but not for taking photographs of other students. Must be closely monitored.	Not allowed
Taking photographs or videos on school's devices.	Allowed with permission	Allowed
Use of hand-held devices such as PDA's, MP3 players	Not allowed. Must be handed in on arrival to school.	Not allowed
Use of personal email addresses in school	Not allowed	Allowed at certain times
Use of online chat rooms in school	Not allowed	Not allowed
Use of instant messaging services	Not allowed	Allowed at certain times
Use of blogs, wikis, podcasts	Allowed within learning activities under staff guidance and supervision	Allowed within guidance provided.
Use of video conferencing or other online meetings	Allowed within learning activities under staff guidance and supervision	Allowed for professional purposes