Blatchington Mill School

ONLINE SAFEGUARDING POLICY

Date Policy Created:
Date of last amendment:
Date to be reviewed:

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and governors
- Identify and support groups of students that are potentially at greater risk of harm online than others
- 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 **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

2. Legislation and guidance

2.1 Department for Education

This policy is influenced by a variety of legislation, as well as being 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 cyber-bullying: 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.

2.2 Education Act

This policy also 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 (see Section 6.3 on Examining electronic devices).

The policy also takes into account the National Curriculum computing programmes of study.

2.3 Other relevant legislation

- Data Protection Act 2018 **and General Data Protection Regulation (GDPR)** - Sets out how personal data is to be protected and only used for the intended purpose when shared.
- The Computer Misuse Act - Makes it an offence to:
    - access computer material without permission; e.g. looking at someone else's files
    - access computer material without permission and with intent to commit criminal offences; e.g. hacking into your bank's computer and increasing the money in your own account
    - alter computer data without permission; e.g. writing a virus to destroy someone else's data
- Sexual Offences Act 2003 - Defines and determines the severity of all sexual offences in the UK, including the offence of sexual grooming.
- Malicious Communications Act 1988 - Makes it an offence to send a communication with the intention of causing distress or anxiety.
- Communications Act 2003 Section 127 - Makes it an offence to send an electronic message that is grossly offensive or of an indecent, obscene or menacing character.

3. Roles and responsibilities

3.1 The governing board

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

The governing board will ensure staff:

- undergo online safety training as part of child protection and safeguarding training
- understand their expectations, roles and responsibilities around filtering and monitoring
- 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 board will coordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

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 Department for Education (DfE) filtering and monitoring standards, and discuss with Network Services 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 Ms E Gibson.

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's information and communication technology (ICT) systems and internet (Appendix 1)
- 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 special educational needs and/or disabilities (SEND. See Section 14). 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

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 (DSL)

Details of the school's designated safeguarding lead (DSL) and deputies (DDSLs) 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 every two years 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 services systems manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, network services systems manager 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 child protection policy
- Ensuring that any online safety incidents are logged (by the Year Office teams onto CPOMS, our Child Protection Online Monitoring System) and dealt with appropriately in line with our policies
- Ensuring that any incidents of cyberbullying are logged and dealt with appropriately in line with the behaviour policy, via the Year Office team

- Updating and delivering staff training on online safety (Appendix 2 contains a self-audit for staff on online safety training needs)
- 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
- 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 services systems manager

The network services systems 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 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 security checks and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

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 (Appendix 1), and ensuring that students follow the school's terms on acceptable use.
- 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 reporting them to the DSL and Network Services, as well as the relevant Year Office (if any students are involved with the system failure).
- Following the correct procedures by requesting access from Network Services, 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 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 Families

We support and encourage a partnership approach with families. 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 school's ICT systems and internet (Appendix 1)

Families 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
- Parent resource sheet – Childnet

For a more detailed list of resources, please see Section 15

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 (Appendix 1).

4. Educating students about online safety

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

All schools have to teach Relationships and sex education and health education in secondary schools.

In **KS3 (Years 7, 8 and 9)**, 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 **KS4 (Years 10 and 11)** 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 that 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
    - 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 that 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 form tutor programs and 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 (see Section 13 below).

5. Educating families about online safety

The school supports raising families' awareness of internet safety through this policy and, in particular, with further reading in Section 15.

Parents/carers can request further information on:

- the school systems used to filter and monitor online use
    - Smoothwall, a web content filtering, safeguarding and internet security platform used in schools, and
    - SENSO, a software package for network, classroom, safeguarding and asset management
- 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

Any queries or concerns in relation to online safety or this policy can be raised with any member of staff, but ideally these should be raised with the students' Year Office in the first instance.

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 our school behaviour 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. This will be done through a combination of work in personal, social, health education (PSHE), form tutor time activities, year group assemblies, as well as in computer science lessons. Teaching staff are encouraged to find opportunities to use other aspects of the curriculum to cover cyberbullying in subjects where appropriate.

All staff, governors and volunteers (where appropriate) can access training on cyberbullying, its impact and ways to support students, as part of safeguarding training (see Section 11).

In relation to a specific incident of cyberbullying, the school will follow the processes set out in our 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.

Families can learn more about general E Safety, including cyberbullying, so they are aware of the signs, how to report it and how they can support children who may be affected through organisations and websites listed in Section 15.

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 can seek advice from headteacher, deputy headteacher and/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 cooperation

Members of SLT and Year Office teams 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 DSL and headteacher or 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 student and/or the parent/carer refuses to delete the material themselves

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 Dealing with Nudes

As suggested by the DfE, the school acts on the assumption that there is always the potential of online sexual abuse - even when we do not have specific information suggesting it is an issue.

- The school does not only rely upon student reporting - all members of staff are proactive in preventing and looking out for the early signs
- The PSHE curriculum details the actions taken after a disclosure is made, so students are aware of what might happen when they talk to an adult in school about online sexual abuse

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 and ensure it is not shared further
- Confiscate the device and report the incident to the DSL 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

6.5 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.

Blatchington Mill School 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. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Blatchington Mill School will treat any use of AI to bully students 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 should carry out a risk assessment where new AI tools are being used by the school.

7. Acceptable use of internet in school

All users of our ICT systems, including students, families, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems (Appendix 1). Visitors will also 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 and restrict access through filtering systems where appropriate. Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

More information is set out in the acceptable use agreement in Appendix 1.

8. Social networks

All members of the school community should bear in mind that the information they share through social networking applications, even if they are on private spaces, may be subject to copyright, safeguarding and data

protection legislation. Everyone is to operate in line with the relevant school policies on equalities, harassment, child protection, safer recruitment, and online safety and ICT acceptable use, whether during school hours or otherwise.

8.1 Social media

For the purposes of this document, 'social media' is considered to include all technologies that allow individuals to communicate and share information (including photos and video). Examples include: Facebook, Snapchat, Instagram, WhatsApp, X, YouTube, TikTok, KIK, Flickr, Tumblr, forums, bulletin boards, multiplayer online gaming, chatrooms, Instant Messenger, video conferencing platforms, and many others.

- The school will block/filter access to social networking and newsgroup sites other than those approved by the school for use in school.
- Official school social media posts, blogs or wikis will be password protected and run within the school.
- We would ask that everyone in our school community is respectful of others and posts reflect the values and ethos of the school.
- Students are advised:
    - never to give out personal details which may identify them and/or their location. Examples include real name, address, mobile or landline phone numbers, school attended, email addresses, full names of friends, specific interests and clubs etc.
    - not to place personal photos on social network spaces without due consideration and regard to background detail in a photograph which could identify the student or location (e.g. house number, street name or school).
    - on security, and encouraged to set strong passwords, to deny access to unknown individuals and instructed how to block unwanted communications.
    - to only invite or accept known friends and deny access to all others.
    - that allowing access to a friend on their social network space could allow access to friends of that friend, who would be unknown to the student.
    - not to publish specific and detailed private thoughts.
- Staff are advised **not** to:
    - run social network spaces for student use on a personal basis.
    - befriend, seek to befriend, or communicate with students on any social networking site or outside the official school system.

Staff members should also read our staff Code of Conduct and the Social Networking Policy for Employees of Brighton & Hove City Council as well as staff updates as appropriate (for example through staff emails and staff meetings).

9. Students using mobile devices in school

Mobile phones are not to be used in school by students. This includes anywhere on the school grounds from the start of the school day. Students may bring mobile devices into school, but are not permitted to use them during:

- Lessons

- Break time
- Lunch time
- Tutor group time
- Any time during school hours, without the express permission of staff
- Clubs before or after school, or any other activities organised by the school

Any breach in mobile phone use by students may trigger disciplinary action in line with our school behaviour policy, which may result in the confiscation of their device. Please see our behaviour policy (link in Section 14) for further details.

10. Staff using work devices outside of 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 that 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
- Not using hard drives or memory sticks
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Helping to keep anti-virus and anti-spyware software, as well as operating systems, up to date, by allowing installations of the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in Appendix 1.

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 Network Services.

11. 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 this and our behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

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 staff disciplinary procedures and 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 that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

12. Training

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

All staff members will receive refresher training, 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, threatening, 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
- the ability to ensure students can recognise dangers and risks in online activity, and can assess those risks
- the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and DDSLs 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 and child protection policy and procedures.

13. Monitoring arrangements

The DSL, DDSLs and Year Office will log behaviour and safeguarding issues related to online safety on CPOMS (Child Protection Online Monitoring System).

This policy will be reviewed every two years by the DSL. At every review, the policy will be shared with the governing board. The review will be supported by a risk assessment (such as the one available here) that considers and reflects the risks students face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

14. SEND

14.1 Education and training

When teaching about online safety, learners with special educational needs and/or disabilities (SEND) may need:

- complex online safety issues to be broken down and explained in other ways
- to explore issues in a variety of contexts and approaches (e.g. cause and effect)
- more examples of safe and unsafe practices
- extra reinforcement and repetition of key safety messages
- differentiated teaching resources and materials
- more engagement with families, as they play a vital role in supporting children to learn how to be safe online

14.2 Reporting concerns

Learners with SEND may require a range of methods to enable them to report concerns and seek support. Example include:

- Non-verbal learners may require a messaging or sound system on their devices to help them to get adult attention
- Learners may have 1-2-1 workers or trusted adults that they prefer to speak to who will be able to support the DSL in communicating with the learner

15. Links with other policies

This online safety and safeguarding policy is linked to our:

- Safeguarding and child protection policy and procedures
- Behaviour policy
- Anti-bullying policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

16. Online Safeguarding Contacts and References

- General Advice on Staying Safe Online
    - Childline - http://www.childline.org.uk/

- Internet Matters - http://www.internetmatters.org/
- UK Safer Internet Centre - https://www.saferinternet.org.uk/ (Helpline for professional)
- NSPCC - https://www.nspcc.org.uk/keeping-children-safe/online-safety
- Think U Know website - http://www.thinkuknow.co.uk/
- Digital Parenting - https://parentzone.org.uk/

- Reporting
  - Child Exploitation & Online Protection Centre - https://www.ceop.police.uk/safety-centre/
  - Childnet International - http://www.childnet.com
  - Internet Watch Foundation - http://www.iwf.org.uk/ (Anonymously)
- Remove Nude or Sexual Contents
  - Internet Watch Foundation - http://www.iwf.org.uk/ (Anonymously)
  - Childline - https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/report-remove/
- Cyberbullying Guidance
  - Childnet - https://www.childnet.com/resources/cyberbullying-guidance-for-schools/

Appendix 1 - Acceptable use policy for the school's ICT systems and internet

The Acceptable Use Policy (AUP) is found on school Microsoft desktops in the form of popups every seven days. If any user (including students, staff, governors, visitors, etc) does not accept the conditions, the system will not open for the individual to use.

The terms of the Acceptable Use Policy are as follows:

- All users, including students and staff, have access to the school ICT systems on the understanding that they accept the terms laid out in this 'Acceptable Use Policy for the School's ICT Systems' document.
- Access must only be made via your authorised login and password. Your password must not be made available to any other person.
- All internet use should be appropriate to staff professional activity or student's education and learning.
- Activity that threatens the integrity of the school ICT systems, or that attacks or corrupts other systems, is forbidden.
- Sites and materials accessed must be appropriate to work in school.
- Users are responsible for email that they send and for the contacts they make that may result in email being received.
- Professional levels of language and content should be applied to all forms of digital communications both internal and external.
- Copyright of materials and intellectual property rights must be respected at all times.
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- Students' use of chat rooms, or any other interactive message board is forbidden unless specifically directed by a member of staff.
- Accessing or creating, transmitting, displaying or publishing any material (e.g. images, sounds or data) that is likely to cause offence, inconvenience or needless anxiety is unacceptable.
- Users must ensure they are aware of their own e-safety at all times. The school has published an 'Online Safeguarding Policy" document which is available to any user from the school website.
- Users must not bring the school, or any members of the school community, into disrespect by publishing any form of defamatory material on the internet which is then available for viewing by others.
- The use of mobile devices is only allowed in strict accordance with the terms of our behaviour policy and staff code of conduct.
- The school may check any user's computer files, monitor the internet sites they visit, or inspect their email at any time and without their knowledge.
- If you are unsure of any rules, please seek advice from the Network Services Office.

Appendix 2: Online safety training needs – self-audit for staff

In order to understand our staff training needs, staff will conduct this self assessment when requested via Google form.

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways students can abuse their peers online?	
Do you know what you must do if a student approaches you with a concern or issue?	
Are you familiar with the school's acceptable use policy for students, staff, volunteers, governors and visitors?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyberbullying?	
Are there any areas of online safety in which you would like training/further training?	