Online Safety Policy

Approved by:		**Date:**
Last reviewed on:	April 2023	
Next review due by:	April 2024	

Contents

---

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, 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
- 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

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 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.

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.

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

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 coordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

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 (appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or college 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

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 DSL 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, ICT 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 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

This list is not intended to be exhaustive.

3.4 The ICT Manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, 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 regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are referred to DSL and dealt with appropriately in line with this policy
- Working with the DSL to ensuring that any incidents of cyber-bullying are referred and therefore dealt with appropriately in line with the school behaviour 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 (appendix 3), and ensuring that pupils follow the school's terms on acceptable use as accessed on the log on screen (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged on Bromcom 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.

3.6 Parents

Parents 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 (appendices 1 and 2)

Parents 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 (appendix 3).

Visitors using the 'guest wifi' they are supplied with a one use code and a guest AUP.

4. Educating Pupils About Online Safety

Pupils will be taught about online safety as part of the curriculum at Sharples School:

Through the Computing curriculum:

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

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

Through the PSHE curriculum:

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)

Aspects of online safety will also be covered in other subjects and through our assembly and pastoral programme where relevant. Cross curricular links are considered by all teachers at Sharples School.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND whilst still maintaining teaching of the statutory curriculum for secondary students.

5. Educating Parents About Online Safety

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.

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.

6. Cyber-bullying

6.1 Definition

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

6.2 Preventing and Addressing Cyber-bullying

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

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

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.

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

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.

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

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will 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 pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

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

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher, DSL or Year Coordinator.
- 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

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

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

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent 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 pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation

- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy

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

7. Acceptable Use of the Internet in School

Prior to logging on to the school network or devices, all pupils and staff (as well as any other individual who may have access to school devices) will be presented with an 'Acceptable User Policy' agreement. (appendices 1 and 2). The user must click to confirm their agreement to proceed to the Acceptable Use policy (appendix 3).

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 pupils, 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 appendices 1, 2 and 3.

8. Pupils Using Mobile Devices in School

Pupils may bring mobile devices into school, but are not permitted to use them on the school grounds.

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

9. Staff Using Work Devices Outside School

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

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

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

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

10. How the School will respond to Issues of Misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policy on behaviour. 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 the 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. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying 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 DSLs will undertake child protection and safeguarding training, which will include online safety, at least every 2 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 child protection and safeguarding policy.

12. Monitoring Arrangements

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

This policy will be reviewed every year by the Assistant Headteacher. At every review, the policy will be shared with the governing board.

13. Links with Other Policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

Appendix 1: Acceptable Use policy agreement: Staff

The school provides computer systems to users as an important tool for teaching, learning, and administration of the school. Users have a responsibility to use the school's computer systems in a professional, lawful and ethical manner. Deliberate abuse of the school's computer systems may result in disciplinary action (including possible criminal liability). Please note that use of the school computer systems are intended to be as permissive and flexible as possible under current UK legislation, GDPR and DfE guidelines. This policy is not intended to arbitrarily limit the ways in which you can use the system, but to ensure compliance with the legal responsibilities of the users, to safeguard the reputation of the school, and to ensure the safety of all users. Only access the computer systems with Username and Passwords provided to you. Under no circumstances should user accounts or sessions be shared. By accessing the computer systems you are agreeing to the school's Acceptable Use Policy which is available to you in the following locations. For staff see "Operational Staff Resources (M:)" & Staff Central. For students see "Student Resources (L:)". For visitors, you will be presented with the school's Acceptable Use Policy after login. Alternatively please contact IT Support.

Appendix 2: Acceptable Use policy agreement: Pupils

The school provides computer systems to users as an important tool for teaching, learning, and administration of the school. Users have a responsibility to use the school's computer systems in a professional, lawful and ethical manner. Deliberate abuse of the school's computer systems may result in disciplinary action (including possible criminal liability). Please note that use of the school computer systems are intended to be as permissive and flexible as possible under current UK legislation, GDPR and DfE guidelines. This policy is not intended to arbitrarily limit the ways in which you can use the system, but to ensure compliance with the legal responsibilities of the users, to safeguard the reputation of the school, and to ensure the safety of all users. Only access the computer systems with Username and Passwords provided to you. Under no circumstances should user accounts or sessions be shared. By accessing the computer systems you are agreeing to the school's Acceptable Use Policy which is available to you in the following locations. For staff see "Operational Staff Resources (M:)" & Staff Central. For students see "Student Resources (L:)". For visitors, you will be presented with the school's Acceptable Use Policy after login. Alternatively please contact IT Support.

Appendix 3: Acceptable Use policy document (all users)

Acceptable Use Policy (AUP)

Computer Systems for All Users

1. Guidelines for Users

The school has provided computers for use by users as an important tool for teaching, learning, and administration of the school. Use of school computers and laptops is governed at all times by the following policy. Please ensure you understand your responsibilities under this policy, and direct any questions or concerns to the Network Manager in the first instance.

All users have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. Deliberate abuse of the school's computer system may result in disciplinary action and civil and/or criminal liability.

The school recognises that the distinction between computer use at work and at home is increasingly blurred, with many of us now using our own computers for work. Users should consider that this policy applies whenever you are undertaking an activity that relates to the school.

2. Computer Security and Data Protection

a) You will be provided with an account for accessing the computer system. This account will be tailored to the level of access you require, and is for your use only. As such, you must not disclose your password to anyone, including IT support staff.
b) You must only login with the account details that have been provided to you. Under no circumstances should user accounts be shared for any length of time, even if supervised. c) When leaving a computer unattended, you must ensure you have either logged off your account, or locked the computer (eg. by pressing the WINDOWS key + L) to prevent anyone using your account in your absence.
d) You must not store any sensitive or personal information about staff or students on any device (such as a USB memory stick, portable hard disk, personal computer etc.) unless that storage system is encrypted and approved for such use by the school. e) To ensure data is safely backed up, it must be stored centrally on the school network. This is the safest place to store data to minimize the risk of accidental loss of information. f) You must ensure that items of portable computer equipment (such as laptops, digital cameras, or portable projectors) are securely stored in a locked room or cupboard when left unattended.

g) School-related sensitive and confidential material should only be printed to printers with the print release function or in areas that aren't accessible to other individuals. Print jobs released from these print release terminals should also be supervised at all times until the print job has been completed.

3. Personal Use

The school recognises that occasional personal use of the school's computers is beneficial both to the development of your IT skills and for maintaining a positive work-life balance. Such use is permitted, with the conditions that such use
a) must comply with all other conditions of this AUP as they apply to non-personal use, and all other school policies regarding user conduct;
b) must not interfere in any way with your other duties or those of any other member of staff; c) must not have any undue effect on the performance of the computer system; and d) must not be for any commercial purpose or gain unless explicitly authorized by the school. Personal use is permitted at the discretion of the school and can be limited or revoked at any time.

4. Use of your own Equipment

a) Any mains-operated personal computer or electrical equipment brought on site, for any use, maybe subject to a Portable Appliance Test (PAT). This test must be performed at regular intervals as required by school's normal rules on electrical safety testing. b) You must not connect personal computer equipment to school networked computers without prior approval from Network Manager, with the exception of storage devices such as USB memory sticks and personal digital cameras.
c) If you keep files on a personal storage device (such as a USB memory stick or harddrive), you must ensure that other computers you connect this storage device to (such as your own computers at home) have an up-to-date anti-virus system running to protect against the proliferation of harmful software onto the school computer system.

5. Conduct

a) You must at all times ensure your computer usage is professional, ethical and lawful, which includes being polite and using the system in a safe, legal and business appropriate manner. Among the uses that are considered unacceptable are the following: • Using, transmitting, or seeking inappropriate, offensive, pornographic, vulgar, suggestive, obscene, abusive, harassing, threatening, racist, sexist, or defamatory language or materials;
• Making ethnic, sexual-preference, or gender-related slurs or jokes.
• along with any other behavior that the school deems inappropriate.
b) You must respect, and not attempt to bypass, security or access restrictions in place on the computer system.
c) You must not intentionally damage, disable, or otherwise harm the operation of computer systems and other hardware.
d) You must make efforts not to intentionally waste resources. Examples of resource wastage include:
o Excessive downloading/streaming of material from the Internet;
o Excessive storage of unnecessary files on the network storage areas;

o Excessive use of printers.
e) You should avoid eating or drinking around computing equipment.

6. Use of Social Media and online forums

Users must take care when using social media websites and apps such as Facebook, Twitter, Instagram, Snapchat, even when such use occurs in their own time using their own computer. Social media sites invite users to participate in informal ways that can leave you open to abuse, and often make little or no distinction between adult users and children. a) Staff must not add a pupil to your 'friends list'.
b) Staff must ensure that personal information is not accessible via a 'Public' setting, but ensure it is set to a 'Friends only' or equivalent level of visibility.
c) Staff should avoid contacting any pupil privately via a social media website, even for school-related purposes.
d) You should take steps to ensure that any person contacting you via a social media website is who they claim to be, and not an imposter, before allowing them access to your personal information.
e) Staff should also take care when posting to any public website (including online discussion forums or blogs) that their comments do not harm their professional standing or the reputation of the school – even if their online activities are entirely unrelated to the school.
f) Misuse of online activities, in school or outside of school, can lead to disciplinary action being taken by the school.
g) Unless authorised to do so, you must not post content on websites that may appear as if you are speaking for the school.
h) You should not post any material online that can be clearly linked to the school that may damage the school's reputation.
i) You should avoid posting any material clearly identifying yourself, another member of staff, or a pupil, that could potentially be used to embarrass, harass, or defame the subject. j) You must adhere to any further social media policies from the school.

7. Use of Email

All users with a computer account who have been provided with an email address for communication. The following considerations must be made when communicating by email: a) E-mail has the same permanence and legal status as written hardcopy (paper) documents and may be subject to disclosure obligations in exactly the same way. Copies of e-mails may therefore have to be made available to third parties. You must be cautious when sending both internal and external mails. The professional standards that apply to internal memos and external letters must be observed for all e-mail.
b) E-mail to outside organisations has the same power to create a binding contract as hardcopy documents. Check e-mail as carefully as written contracts, always use a spell checker and, where appropriate, obtain legal advice before sending. You must not purchase goods or services on behalf of the school via e-mail without proper authorisation.

c) E-mail is not a secure method of communication, and can be easily copied, forwarded and archived. Unless explicitly authorised to do so, you must not send, transmit, or otherwise distribute proprietary information, copyrighted material, trade secrets, personal data or other confidential

information belonging to the school.
d) Having an external e-mail address may lead to receipt of unsolicited e-mail containing offensive and/or sexually explicit content. The school will take measures to minimise the receipt and impact of such content, but cannot be held responsible for material viewed or received by users from the Internet.
e) You must not send chain letters or unsolicited commercial e-mail (also known as SPAM). f) If you are signing up to an officially sanctioned service you must use your provided school email address.
g) Any provided school email accounts, must not be used for personal use. This includes signing upto 3rd party systems or services.
h) Access to the provided school email account, can be terminated at anytime and will be once your employment/enrollment has ended.

8. Supervision of Pupil Use

a) When arranging use of computer facilities for pupils, you must ensure supervision is available.
b) Supervising staff are responsible for ensuring that the Acceptable Use Policy is enforced.

9. Privacy

a) Use of the school computer system, including your email account and storage areas provided for your use, may be subject to monitoring by the school to ensure compliance with this Acceptable Use Policy and applicable laws. This may include remote monitoring of an interactive logon session. In particular, the school does keep a complete record of sites visited on the Internet by both pupils and staff, however, usernames and passwords used on those sites are NOT monitored or recorded.
b) You should avoid storing non-school related data on the school computer system that is unrelated to school activities (such as personal passwords, photographs, financial information etc.).
c) The school may also use measures to audit the use of computer systems for performance and diagnostic purposes.
d) Use of the school computer system indicates your consent to the above described monitoring taking place.

10. Confidentiality and Copyright

a) Respect the work and ownership rights of people outside the school, as well as other staff or pupils.
b) You are responsible for complying with copyright law and licenses that may apply to software, files, graphics, documents, music, messages, and other material you wish to use, download or copy. Even if materials on the school computer system or the Internet are not

marked with the copyright symbol (©), you should assume that they are protected under copyright laws unless there is an explicit permission on the materials to use them. c) You must consult the Network Manager before placing any order of computer hardware or software, or obtaining and using any software you believe to be free. The installation of freemium or trial software will not be

permitted. This is to check that the intended use by the school is permitted under copyright law (as well as to check compatibility and discuss any other implications that the purchase may have). Do not rely on the claims of suppliers, who do not have specific knowledge of the school's systems.
d) You must adhere to any GDPR policies from the school.

11. Reporting Problems with the Computer System

It is the job of the Network Manager to ensure that the school computer system is working optimally at all times and that any faults are rectified as soon as possible. To this end: a) You should report any problems that need attention to a member of IT support staff as soon as is possible. Problems that seriously hinder your job or teaching and require immediate attention should be reported by telephone; any other problem must be reported via email.
b) If you suspect your computer has been affected by a virus or other malware, you must report this to a member of IT Support staff immediately.

12. Reporting Breaches of this Policy

All users have a duty to ensure this Acceptable Use Policy is followed. You must immediately inform a member of the IT Support staff, or the SLT, of abuse of any part of the computer system. In particular, you should report:
a) any websites accessible from within school that you feel are unsuitable for staff, student or visitor consumption;
b) any inappropriate content suspected to be stored on the computer system. This may be contained in email, documents, pictures, etc;
c) any breaches, or attempted breaches of computer security; or
d) any instance of bullying or harassment suffered by you, another user via the school computer system.

Reports should be made to a senior member of staff. All reports will be treated confidentially.

13. Availability and Reliability

Sharples School makes no representations or warranties concerning the availability or security of the non-domain computers or WiFi networks, and all use is provided on an as-is basis. Sharples School reserves the right to disconnect any user at any time and for any reason. Users will not be given permission to install any software on our computers or access any of our network shares. Sharples School takes no responsibility and assumes no liability for any content uploaded, shared, transmitted, or downloaded by you or any third

party, or for anything you may encounter or any data that may be lost or compromised whilst using the computer networks.

14. Review and Evaluation

This policy will be reviewed regularly and in response to any changes affecting the basis of the original risk assessment, for example: significant security incidents, new vulnerabilities and

significant changes to the organisation or technical infrastructure.

15. Notes

"Sensitive personal information" is defined as information about an individual that is protected by law. An exact definition can be found in GDPR under the title of “special category data”. Examples of such data include addresses and contact details of individuals, dates of birth, and pupil SEN data. This list is not exhaustive.

When this policy was reviewed, an equality impact assessment was conducted to ensure any changes did not have an adverse effect under the terms of the Equality Act 2010. Should you have any comments regarding this policy, please contact the school.