E SAFETY POLICY

incorporating Computer Acceptable Use (Pupil) and Social Networking Policies

Committee Responsible: **School Life Sub-Committee (DF)**

Reviewed by: **Head of Junior School**
(names)

Adopted by Committee: **June 2021**
(date)

Last reviewed: **June 2023**
(date)

Date of next review: **June 2025**

Contents

1 Introduction

1.1 Writing and reviewing

This policy takes into account guidance from the DfE including Keeping Children Safe in Education (KCSIE 2023), ISI, ISBA and other appropriate organisations. It is published on our school website; further copies are available to parents and pupils on request.

1.2 Why a policy?

Internet enabled devices are vital tools for modern education; they are an essential part of everyday life for academic work and social interaction both in and out of school. We therefore have a duty to provide pupils and staff with quality internet access as part of their learning experience. We also have a responsibility to ensure that, from a young age and as part of their broader education, pupils understand the inherent risks, and learn how to evaluate online information and how to take care of their own safety and security in the digital world. The use of the latest technology is actively encouraged at Sibford School but with this comes a responsibility to protect pupils, staff and the school from abuse of the system. The school system has appropriate firewalls and filters to prevent access to unsuitable websites.

Internet use at Sibford School is intended to enhance and enrich teaching and learning, to raise educational standards and promote pupil achievement, to develop initiative and independent learning by providing access to information and to alternative viewpoints, to foster imagination and stimulate intellectual curiosity, and to support the professional work of staff and enhance the school's management functions. For boarders, and in particular international boarders, internet enabled devices are a crucial means of keeping in touch with home and family.

1.3 Policy Aims

- To enable pupils to take full advantage of the educational opportunities provided by e-communication;
- To ensure that, as a school, we work to develop in pupils the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies, both in and beyond the classroom;
- To inform and educate pupils as to what constitutes appropriate and inappropriate internet usage;
- To inform and educate pupils as to what constitutes appropriate and inappropriate device usage;
- To safeguard pupils from potentially harmful and inappropriate online material, including extremist material and ideology, by ensuring that appropriate filtering and monitoring systems are in place;
- To protect pupils from cyberbullying and abuse of any kind derived from e-sources;
- To inform pupils of what to do if they come across inappropriate material or are concerned about online activity;
- To help pupils to understand the range of risks inherent in the digital world – including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking and abuse - and to take responsibility for their own online safety;
- To ensure that the copying and subsequent use of internet-derived materials complies with copyright law;
- To help protect the interests and safety of the whole school community and to provide guidance on how, as a school, we will deal with any infringements.

2 Scope

2.1 This policy covers both fixed and mobile internet devices provided by the school (such as PCs, laptops, tablets, electronic whiteboards, webcams, digital video equipment, etc.) as well as all devices owned by pupils and staff brought onto school premises (such as personal laptops, tablets, smart phones, etc.) and extends to inappropriate use off site.

It is linked to a number of other school policies and protocols including:

- Safeguarding (Child Protection) Policy
- Social Respect Policy
- Behaviour Policy
- Employment Procedures and Staff Code of Conduct
- Data Protection Policy
- Health and Safety Policy

- Curriculum Policy
- Computer Acceptable Use Policy for Staff

3 Definitions

3.1 E-Safety means limiting the risks to which pupils and staff are exposed when using the internet and associated technologies, so that all such technologies are used safely and securely and with a clear understanding of the range of potential risks that could be inherent in their use.

4 Guidelines

4.1 Application
Sibford School's E-Safety Policy applies to day pupils and boarders. It is interpreted and applied age-appropriately.

4.2 Responsibility for E-safety at Sibford School.
In as much as E-Safety is part of the broader context of Safeguarding, issues relating to E-Safety at Sibford School fall within the scope of the responsibilities of all members of staff to varying degrees and to all members of staff with roles in school.

For further details please refer to the Safeguarding (Child Protection) Policy.

4.3 Pupil responsibility
Protecting hardware via mediums such as filters and firewalls and the vigilance of teachers and parents, have an important part to play in the safeguarding and protection of pupils both at school and at home. However, young people have wide ranging access to the internet, so the most effective form of protection ultimately lies in the good sense of young people and in exercising judgement guided by a well-informed understanding of what is available to them and of the risks to which they are potentially exposed.

For this reason, we work on the basis that pupils must be responsible for their own actions, conduct and behaviour when using the internet.

Use of technology should be safe, responsible, and legal. Any misuse of the internet, inside or outside of school, will be dealt with under Sibford School's Behaviour Policy and/or Safeguarding (Child Protection) Policy.

Sanctions will also be applied to any pupil found to be responsible for any material on his or her own or another website or social media networking site, that would constitute a breach of school rules in any other context.

Access to the internet in school is given to pupils on the understanding that they will use it in a considerate and responsible manner. It may be withdrawn if acceptable standards of use are not maintained.

4.4 Filtering and monitoring

The internet has become a significant component of a number of key safeguarding issues including pornography, child sexual exploitation, predation and radicalisation. Schools have a duty and a responsibility to limit children's exposure to such risks on their IT systems. As part of this process, we have in place a filtering and monitoring system which is designed to comply with the latest government guidance. The system is applied in an age-appropriate way and, in line with the guidance in KCSIE 2020, with the aim of ensuring that it does not, through 'over blocking', lead to unreasonable restrictions being imposed on what pupils can be taught with regards to online teaching and safeguarding.

4.5 Monitoring and usage

Users should be aware that the school can track and record the sites visited and any searches made on the internet by individual users. We would advise parents that we provide filtered access to the internet for pupils, but they should also be aware that, with emerging and constantly changing technologies, there is no absolute guarantee that a pupil will not be able to access material that would be considered unsuitable through the use of internet enabled devices with 4G. The chance of just coming across such content is highly unlikely, but it obviously increases in direct proportion to the amount of time and effort an individual puts into their search. Anyone inadvertently coming into contact with such material must contact a member of staff immediately.

4.6 Social Respect

Pupils must not use their own or Sibford School's devices and technology to intimidate others either inside or outside the confines of school buildings. Incidents involving the use of technology will be dealt with under Sibford School's Behaviour/Social Respect Policies.

4.7 Abuse

If there is a suggestion that a pupil is at risk of abuse from his or her involvement in any form of online activity, including the risk of radicalisation and being drawn to extremist organisations of ideology, the matter will be dealt with under Sibford School's Safeguarding (Child Protection) Policy. If a pupil believes a fellow pupil to be a victim or perpetrator of any internet/e-safety based behaviour or is worried about something that they have seen on the internet, they should report it to a member of staff immediately.

4.8 Responses

- All E–safety complaints and incidents will be recorded on SIMS, together with actions taken.
- Breaches of regulations will be dealt with according to Sibford School's Behaviour and Safeguarding (Child Protection) Policies.
- Intimidation in any form, including cyberbullying, is wholly unacceptable at Sibford School. Any instances of cyberbullying will be taken very seriously and dealt with thoroughly and appropriately in accordance with Sibford School's Behaviour/Social Respect Policies.
- Where there is reasonable cause to suspect that a child is suffering, or is likely to suffer, significant harm as a result of intimidation in any form, including cyberbullying, then the matter will be treated as a child protection issue and referred to Children's Social Care and the Police in accordance with the Social Respect and Safeguarding (Child Protection) Policies.

5 Principles and acceptable use of the internet at Sibford

5.1 Password security
Pupils have individual logins to access the school network. It is important that pupils understand and respect the need for password security.
All pupils should:

- Not write their passwords down;
- Never share passwords with other pupils, or adults who are not members of staff.

5.2 Copyright
When using the internet, all users are expected to comply with all laws and government regulations concerning copyright, libel, fraud, data protection, discrimination and obscenity. Any attempt to access material which promotes extremism or radicalisation will be taken very seriously and dealt with immediately as set out in the section on 'The Prevent Duty' in Sibford School's Safeguarding (Child Protection) policy.

5.3 All pupils are expected to behave responsibly on the school computer network. Junior School pupils (including those in EYFS) only have access to the network under adult supervision. No intranet or internet user at Sibford School is permitted to:

- Retrieve, send, copy, share, display or put online any content that is offensive in messages or pictures, including Youth Produced Sexual Imagery (YPSI/sexting) and so-called nude selfies;

- Use obscene, racist, homophobic, pornographic, or otherwise discriminatory language;

- Send, share or in any other way put online any content that is racist, discriminatory, pornographic, conducive to extremism, violence or radicalisation, or in any sense offensive to any other person or group of people, including but not limited to protected characteristics under the Equality Act 2010, or likely to bring the school into disrepute;

- Harass, insult or attack others in school or out;

- Access, or attempt to access, material that promotes extremism and or terrorist activity or organisations, pornography or any other form of harmful, inappropriate or illegal content. If a user finds that they have accessed such content mistakenly, they should inform a member of staff or line manager immediately. If a user is planning an activity which might breach this policy (e.g. research into terrorism for a legitimate project), they should seek permission from a member of staff;
- Damage computers, computer systems or computer networks, including tampering with cables or disconnecting hardware;

- Use another user's password or account;

- Trespass in another user's folders, work or files;
- Use the network for commercial purposes;
- Download and install software or install hardware onto a school computer, whether legitimately licensed or not, including knowingly distributing a virus;
- Intentionally waste limited resources, including printer ink and paper;
- Use the school computer system or the internet for private purposes unless the Head or other senior member of staff has given express permission for that use.
- Copy, save or redistribute copyright-protected material without approval;
- Subscribe to any services or ordering any goods or services unless specifically approved;
- Plagiarise the ideas, information or writing of others found on the internet or anywhere else. This could result in disqualification from exams in case of coursework;
- Play computer games unless specifically approved by the school;
- Publish, share or distribute any personal information about any other user such as home address, email address, telephone number, photographs etc;
- Use internet chat rooms;
- Use the network in such a way that its use by other users is disrupted (for example: downloading large files during peak usage times; sending mass email messages);
- Bypass or attempt to bypass any of the school's security or monitoring systems for example, by setting up a Virtual Private Network (VPN);
- Any activity that violates a school rule.
- Use email or the internet during lessons unless a member of staff has given permission.

5.4 Managing Email

Email is the *sine qua non* of modern life and an immensely valuable tool for educational communication. However, it can also be a channel for cyberbullying, abuse and defamation. Spam, phishing and virus attachments can also make email dangerous.

As a consequence:

- Pupils should only use approved email accounts to communicate with staff/other pupils during school time;
- Pupils must notify a member of staff immediately if they receive offensive email;
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone not known to them;
- Pupils should not assume any email sent on the internet is secure;
- Social email use during the school day can interfere with learning and is discouraged;
- Sending or replying to anonymous messages and chain letters is not permitted;

5.5 Managing Social Media and Social Networking sites

- The school will control access to social media and social networking sites because of the potential for harm inherent in such sites.
- Pupils are advised never to give out personal details of any kind which may identify them and / or their location. Examples include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs, etc.
- Pupils are advised not to place personal photos on any social network space. They should think about how public the information is and consider using private areas.
- Pupils are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful, or defamatory. Posts that, in the reasonable opinion of Sibford School, could be deemed offensive or defamatory to individuals or to the school will be regarded as a serious breach of discipline and will be dealt with in the context of Sibford School's Behaviour/Social Respect Policies.

5.6 Managing mobile devices and other electronic equipment

- Senior School pupils in Years 10-13 are permitted to bring mobile devices onto school premises but they remain the responsibility of their owners at all times. The school cannot be held responsible for any theft, loss of, or damage to, such devices suffered on school premises. Pupils in Year 10 and 11 should not use their mobile devices while at school. Pupils in 6th Form may use their mobile devices while in the 6th Form Centre.
- Excepting those who need them for transport reasons, Senior School pupils in Year 7-9 should not bring mobile devices on to the school premises. Those who do, must hand these in at tutor time in the morning and collect them at the end of the school day or in advance of a trip or fixture.

- Junior School pupils may only bring in mobile devices if they travel on school transport. Devices should be handed in to staff and will be returned at the end of the school day. With agreement with the class teacher and Head of Junior School, a Junior School pupils may use a laptop in school. This will be in special circumstances and following the due protocols.
- Mobile devices must not be switched on or used for any purpose in any lesson, or school trip/sports fixture or other formal school occasion, unless expressly authorised to do so by a member of staff.
- Pupils are permitted to wear smart watches on the understanding that if they are deemed a distraction they may be confiscated.
- Mobile devices may not be used to intimidate, harass or insult any other person inside or outside the school either through voice calls, texts, emails, still photographs or videos. Cyberbullying of this nature will be dealt with in accordance with Sibford School's Behaviour Policy.
- Devices containing inappropriate images will be confiscated and dealt with under the Safeguarding (Child Protection) Policy and may involve the police.
- Any misuse of the internet through mobile devices, such as downloading inappropriate or offensive materials or posting inappropriate comments on social networking sites, will be dealt with in accordance with Sibford School's Behaviour Policy.
- Any unacceptable use of mobile devices will be dealt with in accordance with Sibford School's Behaviour/Social Respect Policies.
- Sibford School reserves the right to confiscate, for a fixed period, the mobile device of any person contravening these protocols and to forbid them from bringing a mobile device into school for any length of time deemed appropriate by the school.
- Mobile devices are not permitted in exam rooms.
- Mobile devices are not permitted in the EYFS department or near EYFS pupils. This includes pupils, staff, parents and visitors.

5.7 Photography and video capture on school premises

- Use of photographic material to harass, intimidate, ridicule or bully pupils, staff members or people not a part of Sibford School, will not be tolerated and will constitute a serious breach of discipline.
- Photographs or videos of any person on school premises or during any part of the school day including trips and transport are strictly prohibited.
- Indecent images taken and sent by mobile devices and other forms of technology (sometimes known as 'sexting') is strictly forbidden by the school and in some circumstances, may be seen as an offence under the Protection of Children Act 1978

and the Criminal Justice Act 1988. Anyone found in possession of such images or sending them will be dealt with in accordance with Sibford School's Behaviour Policy, and will likely involve the Police. If a pupil thinks that they have been the subject of 'sexting', they should talk to a member of staff about it as soon as possible.

- The uploading of images onto social networking or video sharing sites which in the reasonable opinion of the school may be considered offensive or harmful is a serious breach of discipline and will be subject to disciplinary procedures.

- Pupils must allow staff reasonable access to material stored on phones and must delete images if requested to do so in any situation where there is any suspicion such images contravene school regulations. See Sibford School's Safeguarding (Child Protection) Policy on Conducting a Search.

- If the school has reasonable grounds to believe that a phone, camera, laptop or other device contains images, text messages or other material that may constitute evidence of criminal activity, the school reserves the right to submit such devices to the police for examination. (Please see Sibford School's Safeguarding (Child Protection) Policy on Conducting a Search.

- Such misuse of equipment will be dealt with according to the school behaviour policy and may involve confiscation and / or removal of the privilege of bringing such devices into school premises on a temporary or permanent basis.

- **Anti-virus software –** all laptops should have appropriate anti-virus software that is regularly updated.

- **Licenced/unlicenced software, distributing files and Warez –** no computer programmes (executables), MP3s, pornography, copyrighted material or material encouraging radicalisation may be distributed over the network. This includes the sending of files via email, as well as setting up 'servers' on pupils' laptops and using them as a means of sharing software, use a VPN. Pupils should not download copyrighted material.

- **School Hardware** – Pupils must not tamper with school computing hardware in any way. This includes attaching and detaching cables, keyboards and computer mice. Nor should school hardware be unplugged. Settings on school hardware must not be altered or personalised. The user of a device should ensure that they log off at the end of a session and shut down the device at the end of the day.

- **'Chatting'** – pupils may not use any chat or collaboration program to communicate with others through the school's computer network unless a member of staff expressly permits them to do so. This includes the use of email during lessons.

- **Audio** – because computer audio can be distracting, the volume setting on laptops must generally be turned off when used during school time.

- **Headphones** – headphones may be permitted if explicitly required in order to participate in a lesson. Headphones are not permitted for any other purpose. It is not the school policy for permit listening to music as a form of relaxation in lessons.

- **Games –** computer games should never be played in school unless part of a specified homework that is detailed on Firefly or through the Junior School homework portals.
- **Privacy –** the school reserves the right to examine the hard drive on a pupil's personal laptop if there is reasonable suspicion that a computer is being used for inappropriate or dishonourable purposes.
- **School owned laptops / netbooks** – these must only be used under the supervision of a member of staff and must only be used for educational purposes. The uploading of inappropriate material such as images, software and graphics is forbidden and this includes the altering of screen savers and backgrounds.

5.8 Best practice:

- When printing, only print if absolutely necessary and only print one copy; ensure your name appears on every printout.
- Always log off when you have finished using a school computer.
- Save work regularly using sensible file names.
- Be mindful of how much is saved to the school network; users should save to the cloud (OneDrive) where possible.
- Observe health and safety guidelines when using computer equipment.
- Be considerate and polite to other users.

6 Cyberbullying

6.1 Many young people and adults find using the internet and mobile devices a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. When children are the target of cyberbullying via mobiles devices, gaming or the internet, they can often feel very alone, particularly if the adults around them do not understand cyberbullying and its effects. A once safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety.

6.2 It is essential that pupils, staff and parents understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of digital citizens will support innovation and safety.

6.3 The DfE and Childnet have produced resources that can be used to give practical advice and guidance on cyberbullying. Refer to Childnet: cyberbulling guidance for schools.

6.4 Cyberbullying (along with all forms of bullying) will not be tolerated at Sibford School, whether the bullying originates inside or outside school. Activities conducted outside of school premises and outside of school hours that in our opinion constitute cyberbullying will also be covered by this policy. Instances of cyberbullying will be dealt with according to Sibford School's Behaviour/Social Respect Policies or, where relevant, the school's Child Protection - Safeguarding Policy. All incidents of cyberbullying reported to the school will be recorded.

6.5 The school will take reasonable steps to identify the person(s) responsible for any instances of cyberbullying such as examining system logs, identifying and interviewing possible witnesses and contacting the service provider and the Police if necessary.

7 E-Safety measures for boarders

7.1 Whilst the E-Safety Policy applies to all members of the Sibford School community, including both day and boarding pupils, there are a number of extra e-safety procedures that are put in place for boarders.

7.2 Sibford School understands that boarders, in a 'home' environment, should have access to social media and other websites one would expect to find on any home-based internet system, whilst also being prevented from accessing material which may cause harm.

7.3 Sibford School also follows guidance from the National Minimum Standards for boarding schools. NMS 4.1 especially recognises that "Boarders can contact their parents/carers and families in private and schools facilitate this where necessary. This does not prevent schools from operating proportionate systems to monitor and control the use of electronic communications in order to detect abuse, bullying or unsafe practice by boarders." With a large percentage of our boarders' parents and carers living abroad, we are aware of the need for boarders to use technology for communication.

7.4 The same protocols are in place for boarders as for day pupils, however, boarding pupils are permitted to access age-appropriate sites for communication in the Boarding Houses.

7.5 In boarding we will also contribute to the safety and security of the boarders by providing information and resources. Posters and leaflets advising on safer use of technology and staying safe online line are prominently displayed in boarding houses. All houseparents are vigilant and monitor boarders' use of technology, looking for any evidence of inappropriate use, harmful online interaction, use of VPNs, signs of addictive behaviour, as well as any other use deemed to be unsafe.

7.6 Boarders understand that this policy applies to them. In addition:

- Boarders are allowed to bring and keep laptops (desktops are prohibited), mobile and other devices. Boarders must declare ALL of these devices to Houseparents who keep a record of them on a central valuables list.
- All boarders in years 7-10 are required to hand in each night all devices which can access the internet. These are collected and stored securely in the office by 10 pm.
- All boarders (years 7-13) understand that boarding house staff may confiscate any device should it be felt that it is affecting their learning, behaviour, sleep pattern or ability to live cohesively in a boarding house.
- The school Wi-Fi shuts down automatically at 11pm every night to ensure they have enough screen-free time before sleep.

- Boarders will be responsible users and stay safe while using the internet and other communications technologies for educational and recreational use.
- The allowances made in boarding for boarders to access certain sites otherwise restricted at school are sympathetic to their needs and that these privileges may be withdrawn if they engage in inappropriate activity.
- Everyone has equal rights to use technology as a resource and the boarding houses computers are intended for educational use and that must take priority.
- That failure to use technology and the internet in an acceptable manner will result in disciplinary action. This may include, but is not limited to, loss of access to the Sibford School Network/ internet, removal of devices, exclusions, and contact with parents and in the event of illegal activities, involvement of the police.

Staff need to be mindful of student's use of technology and whilst the school has a robust filtering system for devices connected to the school's wireless network, it needs to be acknowledged that children can also use a 4G/5G connection to connect to the internet and that this connection may not afford the same safeguards as the school system. In view of this, it is important that all staff make the DSL aware if they become aware or concerned about any inappropriate use of technology.

Students will be supported through the PSHE and Tutorial programmes to help them manage their lives online and keep safe. Years 7-9 also have online security as part of their Programme of Study using the Cyber Explorers resource which is produced in conjunction with the UK Government and GCHQ. The School will also, whenever appropriate, address groups of students and/or parents on specific online issues should the need arise.

The DSL acts as the online safety coordinator and will work with members of the IT Department to ensure that the school is up-to-date with its online provision and protection.

8 Social Networking

8.1 Social Networking applications include but are not limited to blogs, online discussion forums, collaborative spaces, media sharing services, micro-blogging applications, messaging applications. Examples include Twitter, Instagram, Facebook, WhatsApp, Snapchat, YouTube, Tik Tok and can also include instant messaging systems (SMS).

The School recognises that internet Social Networking sites are a useful way of interacting socially with friends and gathering. The School accepts that pupils may use Social Networking applications on the internet. While the School does not wish to discourage acceptable use of such sites, we expect certain standards of conduct to be observed in order to protect:

- The safety, welfare, confidentiality and dignity of staff, pupils, their families and that of the wider community.
- The reputation of the school.

- This policy applies both on and off site. The following principles apply equally to information or comments posted by pupils from their home, personal, school computers or smart devices. This is irrespective of whether the posts are uploaded during school hours or in personal time.
- The pupils are responsible for the content they publish on their Social Media platforms, this policy's primary aim is to provide pupils with guidance to keep them safe and avoid compromising situations which they later regret.
- Current pupils should not be 'friends' with staff on personal Social Networking sites as this could be viewed as a Safeguarding (Child Protection) issue. Pupils may however, 'follow' or 'friend' official School accounts such as, but not limited to, 'Sibford School' on Twitter/Facebook/Instagram.

8.2 Procedure

Pupils must not access Social Networking sites for personal use during the school day, unless otherwise specified by a member of staff.

Use of any Social Media should be age appropriate and pupils should not misrepresent their date of birth in order to gain access to Social Media apps and sites. It is not acceptable to clone someone else's identity or to use a false identity to set up a profile.

Pupils should remember that their profiles on Social Networking sites could directly link their behaviour outside of School with the reputation of Sibford School. Any online conduct that could bring Sibford School into disrepute or cause a negative impact on the school community is forbidden.

Online behaviour that could, in the opinion of Sibford School, cause distress or jeopardise the safety, confidentiality, dignity or reputation of others, whether part of the Sibford School community or not, is not acceptable.

Pupils should take adequate precautions when using Social Networking sites and applications, both in vetting material that could be connected to them (e.g. through their own friendship profiles) and through the appropriate use of security settings. Appropriate security settings should be used to maintain privacy. Social Networking sites which hold personal information and that do not have security settings in place should be avoided.

The pupil's security settings on Social Networking sites should be reviewed regularly as these providers often update their security policies which may allow unauthorised access to the pupil's profile without them being fully aware of such changes.

Pupils should be aware that once content is shared online they lose control of it and it is possible for it to be circulated more widely than intended without prior consent or knowledge (even if content is thought to have been deleted or privately shared).

Pupils should not post/tag comments, photographs, video or other content about any member of the community without their express permission. Sibford School must not be tagged as a location or mentioned in any Social Media posts, blogs, tweets except by official mediums such as Sibford School Twitter or Sibford School Facebook, or Sibford School Instagram.

Sibford School will monitor IT systems and Social Media Sites as is deemed necessary in order to prevent inappropriate usage.

Transcripts of Social Networking communications may be used in any disciplinary proceedings.

If pupils become aware of misuse of Social Networking sites by another pupil, they should inform a member of staff immediately.

Pupils whose conduct breaches this policy in any way may be subject to disciplinary action in accordance with Sibford School's Behaviour Policy.

It should be noted that online behaviour, deemed unsuitable by the Head and in accordance with this policy, may have an impact on a pupil's future relationship with Sibford School. This includes but is not limited to references.

8.3 Sanctions:
In the judgement of the Head, if a pupil is seen to bring Sibford School into serious disrepute, or if a pupil places the welfare, safety, dignity or reputation of others in jeopardy, whether or not they are members of the school community, a period of Fixed Exclusion may result.

In the opinion of the Head, pupils found using Social Media (including email) inappropriately may be sanctioned as follows:

- Required to remove offensive content
- Required to inform their parents/guardians
- Have their internet access temporarily removed (if appropriate)
- Have their free time curtailed
- Pupils with positions of responsibility may lose their posts temporarily or permanently as deemed appropriate by the Head
- Repeat offenders will have a Fixed Exclusion at the discretion of the Head.
- Dependent on the judgement of the Head, a pupil may be excluded permanently.

In such cases, the Head will apply any sanction that is deemed appropriate and proportionate to the breach including, in the most serious cases, asking a pupil to leave the school. Misuse may also lead to confiscation of equipment in accordance with Sibford School's Behaviour/Social Respect Policies.

All infringements will be dealt with in line with the Behaviour/Social Respect Policies.

Sources:
Keeping Children Safe in Education (KCSIE) 2023
'Preventing and tackling bullying - advice for headteachers, staff and governing bodies', October 2017
ISI guidance
EYFS Statutory Framework (2021)
E-safety guidance and model policy issued by the ISBA
Becta www.becta.org.uk/safeguarding
Bristol LA's NGfL Learning Project
CEOP (Child Exploitation and Online Protection Centre www.ceop.police.uk)

This policy should be read in conjunction with the following School Policies:

Behaviour
Safeguarding (Child Protection)
Social Respect
Computer Acceptable Use (Staff)