Online Safety Policy

Date of last review by the DSL | 1 September 2025
Date of next review by the DSL| 1 September 2026

CONTENTS

1	Overview	
1	Aims & Objectives	2
2	Scope	3
3	Roles & Responsibilities	3
2	Legislation and guidance	5
3	Filtering & Monitoring	5
4	Education & Training	6
6	Cyber-bullying	8
7	Use of personal devices	9
8	Online communications	10
10	Use of social media	10
11	Data protection	11
12	Password security	11
13	Safe use of digital video and images	12
14	Artificial Intelligence (AI)	12
15	Misuse	12
16	Acceptable use of the internet at school	13
17	Remote learning	13

APPENDICES

A) Acceptable use agreement (pupils and parents/guardians/carers)
B) Acceptable use agreement (staff, Directors, volunteers, and visitors)
C) Online safety training needs (self-audit for staff)

1 OVERVIEW

1.1 AIMS AND OBJECTIVES

It is the duty of Kew House School to ensure that every pupil in its care is safe; and the same principles apply to the digital world as apply to the real world. Online communications and technology provide opportunities for enhanced learning but also pose great risks to young people. Our pupils are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of bullying, harassment, grooming, stalking, abuse and radicalisation and identity theft.

Technology is continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. However, many information technologies, particularly online resources, are not effectively policed. All users need to be aware, in an age-appropriate way, of the range of risks associated with the use of these internet technologies. Current and emerging technologies used in and outside of school include:

- Websites;
- Email and instant messaging;
- Blogs, forums and chat rooms;
- Mobile internet devices such as smart phones and tablets;
- Social networking sites;
- Music / video downloads;
- Gaming sites and online communities formed via games consoles;
- Instant messaging technology via SMS or social media sites;
- Video calls;
- Podcasting and mobile applications;
- Virtual and augmented reality technology; and
- Artificial intelligence.

This policy, supported by the Acceptable Use Policy (for all staff, visitors and pupils), is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks, deal with any infringements and build online resilience. It is linked to the following school policies:

- Safeguarding and Child Protection Policy
- Staff Handbook
- Behaviour Policy
- Staff Code of Conduct
- RSE Policy
- Acceptable Use of AI

At Kew House School, we understand the responsibility to educate our pupils on online safety issues; teaching them 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 in and beyond the classroom. We also understand the importance of involving pupils in discussions about online safety and listening to their fears and anxieties as well as their thoughts and ideas.

1.2 SCOPE

- This policy applies to all members of the school community, including staff, pupils, parents and visitors, who have access to and are users of the school IT systems. In this policy:
    - “staff” includes teaching and non-teaching staff, directors, and volunteers;

- "parents" includes pupils' carers and guardians; and
- "visitors" includes anyone else who comes to the school.

- Both this policy, and the Acceptable Use policies, cover both fixed and mobile internet devices provided by the school (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.); as well as all devices owned by pupils, staff, or visitors and brought onto school premises (personal laptops, tablets, smart phones, etc.).
- In designing this policy, the school has considered the "*4Cs*" outlined in KCSIE (content, contact, conduct and commerce) as the key areas of risk. However, the school recognises that many pupils will have unlimited and unrestricted access to the internet via mobile phone networks. This means that some pupils, may use mobile technology to facilitate child-on-child abuse, access inappropriate or harmful content or otherwise misuse mobile technology whilst at school. The improper use of mobile technology by pupils, in or out of school, will be dealt with under the school's [Behaviour Policy and / or Safeguarding and Child Protection Policy] as is appropriate in the circumstances.

1.3 ROLES AND RESPONSIBILITIES IN RELATION TO ONLINE SAFETY

All staff, directors and visitors have responsibilities under the safeguarding policy to protect children from abuse and make appropriate referrals. The following roles and responsibilities must be read in in line with the Safeguarding and Child Protection Policy.

1. The Board

The Board has overall leadership responsibility for safeguarding as outlined in the Safeguarding and Child Protection Policy. The Board of the school is responsible for the approval of this policy and for reviewing its effectiveness at least annually.

The Board will ensure that all staff undergo safeguarding and child protection training, both at induction and with updates at regular intervals, to ensure that:

- all staff, in particular the [the IT Manager, Head of Computing, DSL and Senior Leadership Team] are adequately trained about online safety;
- all staff are aware of the expectations, applicable roles and responsibilities in relation to filtering and monitoring and how to raise to escalate concerns when identified;
- staff are aware of the school procedures and policies that should be followed in the event of the abuse or suspected breach of online safety in connection to the school.

2. Headteacher and the Senior Leadership Team

The Headteacher is responsible for the safety of the members of the school community, and this includes responsibility for online safety. Together with the Senior Leadership Team, they are responsible for procuring appropriate filtering and monitoring systems, documenting decisions on what is blocked or allowed and why, reviewing the effectiveness of the filtering and monitoring provisions at least annually, overseeing reports and ensuring staff are appropriately trained.

3. The Designated Safeguarding Lead (DSL)

The DSL takes the lead responsibility for Safeguarding and Child protection at Kew House School. This includes a responsibility for online safety as well as the school's filtering and monitoring system.

The DSL will ensure that this policy is upheld at all times, working with the [Headteacher / Senior Leadership Team], the IT Manager and IT staff to achieve this. As such, in line with the Safeguarding and Child Protection policy, the DSL will take appropriate action if in receipt of a report that engages that policy relating to activity that has taken place online.

The DSL will work closely with the IT Manager and the school's IT service providers to ensure that the school's requirements for filtering and monitoring are met and enforced. The DSL will review filtering and monitoring reports and ensure that regular checks are properly made of the system.

4. IT staff

The school's IT staff have a key role in maintaining a safe technical infrastructure at the school and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of the school's hardware system, its data and for training the school's teaching and administrative staff in the use of IT. They monitor the use of the internet and emails, maintain content filters, and will report inappropriate usage to the DHP & DSL.

5. Teaching and support staff

All staff are required to sign and return the Acceptable Use Policy before accessing the school's systems. As with all issues of safety at this school, staff are encouraged to create a talking and listening culture in order to address any online safety issues which may arise in classrooms on a daily basis.

Teachers must not share the wifi password of KHS Teachers. Sharing of the password may result in disciplinary action.

All staff must read and understand this Online Safety Policy and enforce it in accordance with direction from the Headteacher, DSL or Deputy Head Pastoral (DHP) as appropriate.

6. Pupils

Pupils are responsible for using the school IT systems in accordance with the IT Acceptable Use Policy.

7. Parents and carers

Kew House School believes that it is essential for parents to be fully involved with promoting online safety both within and outside school. We regularly consult and discuss online safety with parents and seek to promote a wide understanding of the benefits and risks related to internet usage. The school will contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school. There will be regular updates to parents via information evenings and the weekly bulletin to raise awareness of digital safety.

2. LEGISLATION AND GUIDANCE

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education - 2025, 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 - for teaching until September 2026
- Searching, screening and confiscation - July 2022

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.

3. FILTERING AND MONITORING

In general:

Kew House School aims to provide a safe environment to learn and work, including when online. Filtering and monitoring are important parts of the school's safeguarding arrangements, and it is vital that all staff understand the expectations, applicable roles and responsibilities in relation to filtering and monitoring.

Staff, pupils, parents and visitors should be aware that the school's filtering and monitoring systems apply to all users, all school-owned devices and any device connected to the school's internet server. Deliberate access, or an attempt to access, prohibited or inappropriate content, or attempting to circumvent the filtering and monitoring systems will be dealt with under the Staff Code of Conduct or the Behaviour Policy, as appropriate.

The school employs a layered approach to safeguarding in the digital environment. **Fastvue reporting with Sophos** is used to monitor, log, and report on network activity, generating alerts for behaviour that may present a safeguarding concern. Alongside this, **Classroom Cloud** is deployed within the computing suites to provide live oversight of pupil activity and to capture keystrokes where required. These measures enable the school to identify, escalate, and address risks promptly, in line with statutory safeguarding obligations and best practice.

This policy will be reviewed every year by the DSL. From January 2022, the reviewed policy has been shared with the Board of Directors. This review will then be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve, and change rapidly.

The IT Manager will review that the filtering and monitoring system are operating effectively. The DHP and DSL will review the filtering and monitoring system, looking at the records of the checks. Such a review should occur before the beginning of every new academic year, however such reviews should occur if:

- there is a major safeguarding incident;
- there is a change in working practices; or
- if any new technology is introduced.

The school's filtering system blocks internet access to harmful sites and inappropriate content. The filtering system will block access to child sexual abuse material, unlawful terrorist content, adult content as well as. If there is a good educational reason why a particular website, application, or form of content should not be blocked a pupil should contact the relevant member of teaching staff, who will then contact the Deputy Head Pastoral or DSL for their consideration.

The school will monitor the activity of all users across all of the school's devices or any device connected to the school's internet server allowing individuals be identified. The IT Manager, DHP and DSL will monitor the logs daily. Any incidents should be acted upon and recorded. If there is a safeguarding concern, this should be reported to the DSL immediately. Teaching staff should notify the DHP or DSL if they are teaching material which might generate unusual internet traffic activity.

Staff:

If any member of staff has any concern about the effectiveness of the filtering and monitoring system, they must report the matter to the DSL immediately in line with the Safeguarding and Child Protection Policy; particularly if they have received a disclosure of access to, or witnessed someone accessing, harmful or inappropriate content. If any member of staff accidentally accesses prohibited or otherwise

inappropriate content, they should proactively report the matter to the DSL or via the self-referral form, accessible via the Staff Intranet.

While the filtering and monitoring system has been designed not to unreasonably impact on teaching and learning, no filtering and monitoring system can be 100% effective. Teaching staff should notify the Head of Department or Deputy Head Academic (DHA) if they believe that appropriate teaching materials are being blocked.

Pupils:

Pupils must report any accidental access to materials of a violent or sexual nature or that are otherwise inappropriate to the DHP or DSL. Deliberate access to any inappropriate materials by a pupil will be dealt with under the school's Behaviour Policy. Pupils should be aware that all internet usage via the school's systems and its Wi-Fi network is monitored.

Certain websites are automatically blocked by the school's filtering system. If this causes problems for school work / research purposes, pupils should contact a member of the teaching staff for assistance.

4. EDUCATION AND TRAINING

1. Staff: awareness and training

As part of their induction, all new teaching staff receive information on online safety, including the school's expectations, applicable roles and responsibilities regarding filtering and monitoring. This will include training on this Online Safety Policy.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following the school's Online Safety procedures.

All teaching staff receive regular information and training (at least annually) on online safety issues in the form of INSET training and internal meeting time, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of online safety.

Teaching staff are encouraged to incorporate online safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the school community. When pupils use school computers, staff should make sure children are fully aware of the agreement they are making to follow the school's IT guidelines.

In accordance with the Safeguarding and Child Protection Policy, if there is a safeguarding concern a report must be made by staff as soon as possible if any incident relating to online safety occurs and be provided directly to the DHP or DSL.

2. Pupils: the teaching of online safety

Online safety guidance will be given to pupils on a regular basis via IS lessons. We continually look for new opportunities to promote online safety and regularly monitor and assess our pupils' understanding of it.

The school provides opportunities to teach about online safety within a range of curriculum areas. Educating pupils on the dangers of technologies that may be encountered outside school will also be carried out via IS, augmented by PT sessions and assemblies, as is appropriate.

At age-appropriate levels, pupils are taught about their online safety responsibilities and to look after their own online safety. Pupils are taught about recognising online sexual exploitation, stalking and grooming, the risks, and of their duty to report any such instances they or their peers come across. Pupils can report concerns to DHP, DSL or any member of staff at the school.

Pupils are also taught about relevant laws applicable to using the internet such as those that apply to data protection, online safety and intellectual property. Pupils are taught about respecting other people's information and images, etc.

Pupils should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the school's Safeguarding / Anti Bullying / Sanctions Policies, which describes the preventative measures and the procedures that will be followed when the school discovers cases of bullying). Pupils should approach the DSL, or any other member of staff they trust, as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies.

3. Parents

The school seeks to work closely with parents and guardians in promoting a culture of online safety. The school will contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

The school recognises that not all parents and guardians may feel equipped to protect their child when they use electronic equipment at home. The school therefore arranges discussion evenings for parents to share updates and good practice; for example, the beginning of year Parent Information Evenings.

5. CYBER-BULLYING

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 one person or group by another person or group, where the relationship involves an imbalance of power. (See also the School Behaviour Policy.)

Preventing and addressing cyberbullying

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. Personal Tutors 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 Individuals in Society lessons, and other subjects where appropriate. All staff, Directors 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 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.

Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the Senior Leadership Team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the Police*

* Staff may also confiscate devices for evidence to hand to the Police, if a pupil discloses that they are being abused and that this abuse includes an online element.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The school's COVID-19 risk assessment

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

6. USE OF PERSONAL DEVICES

Staff

School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. When they are not using a device staff should ensure that it is locked to prevent unauthorised access.

Staff at Kew House School are permitted to bring in personal devices for their own use.

Staff are not permitted under any circumstances to use their personal devices when taking images, videos or other recording of any pupil nor to have any images, videos or other recording of any pupil on their personal devices. Please read this in conjunction with Safeguarding and Child Protection, Acceptable Use, Staff Code of Conduct and School Trips policies. If staff have included pupils in video or images that they have taken, for legitimate reasons, these images must be transferred to the school's storage systems (e.g. OneDrive) and immediately deleted from their personal devices. The self-referral form should be used to log this activity, or the matter raised to the Deputy Head Pastoral or Designated Safeguarding Lead.

Pupils

Pupils are responsible for their conduct when using school issued or their own devices. Any misuse of devices by pupils will be dealt with under the School's Behaviour Policy. The school uses the Yondr system in accordance with the Mobile Phone Policy.

The school recognises that mobile devices are sometimes used by pupils for medical purposes or as an adjustment to assist pupils who have disabilities or special educational needs. Where a pupil needs to use a mobile device for such purposes, the pupil's parents or carers should arrange a meeting with Head of Year to agree how the school can appropriately support such use. The Head of Year will then inform the pupil's teachers and other relevant members of staff about how the pupil will use the device at school.

7. ONLINE COMMUNICATIONS

Staff

Any digital communication between staff and pupils or parents / carers must be professional in tone and content. Under no circumstances may staff contact a pupil or parent / carer / recent alumni (i.e. pupils over the age of 18 who have left the school within the past 12 months) or parents of recent alumni] using any personal email address or SMS / WhatsApp. If this is necessary, the Headteacher must be informed, either in person or via the self-referral form on the Staff Intranet. The school ensures that staff have access to their work email address when offsite, for use as necessary on school business. Personal telephone numbers, email addresses, or other contact details, may not be shared with pupils or parents / carers and recent alumni. Under no circumstances may staff contact a pupil or parent / carer and recent alumni using a personal telephone number, email address, or other messaging system nor should pupils, parents and recent alumni / their parents / carers be added as social network 'friends' or similar.

Staff must immediately report to Headteacher, DHP or DSL if the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to the Headteacher.

Pupils

All pupils are issued with their own personal school email addresses for use on our network and by remote access. Access is via a personal login, which is password protected. This official email service may be regarded as safe and secure, and must be used for all school work. Pupils should be aware that email communications through the school network and school email addresses are monitored.

The school will ensure that there is appropriate and strong IT monitoring and virus software. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for school work purposes, pupils should contact their PT for assistance.

Pupils must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should immediately report such a communication, to a member of staff who should then refer it to the DHP or DSL

8. USE OF SOCIAL MEDIA

Staff

Staff must not access social networking sites, any website or personal email which is unconnected with school work or business from school devices or whilst teaching.

When accessed from staff members' own devices, staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position and the reputation of the school in accordance with the Staff Code of Conduct.

Any online communications, whether by email, social media, private messaging or other, must not:

- place a child or young person at risk of, or cause, harm;
- bring Kew House School into disrepute;
- breach confidentiality;
- breach copyright;
- breach data protection legislation;
- or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:

- making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
- using social media to bully another individual; or
- posting links to or endorsing material which is discriminatory or offensive.

- otherwise breach the Staff Code of Conduct or Child Protection and Safeguarding Policy.

Pupils

The school expects pupils to think carefully before they post any information online orrepost or endorse content created by other people. Content posted must not be, or potentially be, inappropriate or offensive, or likely to cause embarrassment to an individual or others. The school takes misuse of technology by pupils seriously and incidents will be dealt with under the Behaviour, Safeguarding and Child Protection and Anti-Bullying policies as appropriate.

9. DATA PROTECTION

Please refer to the Employment Handbook and the IT Acceptable Use Policy for further details as to the key responsibilities and obligations that arise when personal information, particularly that of children, is being processed by or on behalf of the school.

Staff and pupils are expected to save all data relating to their work to OneDrive.

The school expects all removable media (USB memory sticks, CDs, portable drives) taken outside school or sent by post or courier to be encrypted before sending.

Staff may only take information offsite when authorised to do so, and only when it is necessary and required in order to fulfil their role. No personal data of staff or pupils should be stored on personal memory sticks, but instead stored on an encrypted USB memory stick provided by the school.

Staff should also be particularly vigilant about scam / phishing emails (and similar) which could seriously compromise the school's IT security and/or put at risk sensitive personal data (and other information) held by the school. If in any doubt, do not open a suspicious email or attachment and notify the IT Manager / IT team in accordance with the Data Protection Policy and IT Acceptable Use Policy.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the IT Manager / IT team.

9. PASSWORD SECURITY

Pupils and staff have individual school network logins, email addresses and storage folders on 365. Staff and pupils are regularly reminded of the need for password security.

All pupils and members of staff should:

- use a strong password (usually containing eight characters or more, and containing upper- and lower-case letters as well as numbers), which should be changed every [6] months;
- not write passwords down; and
- not share passwords with other pupils or staff.

10. SAFE USE OF DIGITAL AND VIDEO IMAGES

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own (personal) images on the internet (e.g. on social networking sites) and follow the School's policy on official social media posting.

11. ARTIFICAL INTELLIDENCE (AI)

Any usage by pupils of generative AI tools such as ChatGPT is only permitted in the circumstances acceptable to the class teacher (AI Policy).

In particular, personal or confidential information should not be entered into generative AI tools. This technology can potentially store and/or learn from data inputted and you should consider that any information entered into such tools is released to the internet.

It is also important to be aware that the technology, despite its advances, still produces regular errors and misunderstandings, misinformation, disinformation, conspiracy theories and should not be relied on for accuracy. In particular, pupils should not use these tools to answer questions about health / medical / wellbeing issues, or indeed anything of a personal nature. It is always best to seek help and recommendations as to reliable resources from a member of staff.

Kew House School will evaluate the benefits and risks of any proposed use of generative AI by staff or pupils, with particular regard to risk associated with safeguarding, data protection and the possibility of bias and discrimination. Any approved use of AI will be kept under review and the school will remain alert to the possibility of unauthorised use.

12. MISUSE

Kew House School will not tolerate illegal activities or activities that are in breach of the policies referred to above. Where appropriate the school will report illegal activity to the police and/or the local safeguarding partnerships. If a member of staff discovers that a child or young person is at risk as a consequence of online activity they should report it to the Deputy Head Pastoral or the DSL. The DSL then may seek assistance from the CEOP, the LADO, and/or its professional advisers as appropriate.

Where a pupil misuses the school's ICT systems or Internet, we will follow the procedures set out in our Behaviour and Acceptable Use Policies. 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.

The school will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our Safeguarding and Child Protection and Behaviour policies.

12. ACCEPTABLE USE OF THE INTERNET IN SCHOOL

All pupils, parents, staff, volunteers, and Directors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the Internet (appendices 1-3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

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

We will monitor the websites visited by 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.

13. REMOTE LEARNING

In response to the Covid-19 pandemic the school has used *Microsoft Teams* to deliver learning. In the event of any future Lockdowns, the school will continue to practise the same model of delivering live lessons that mirror the school timetable. Pupils are expected to be at their screens by 8.30 in the morning, dressed appropriately (smart casual) and with all equipment ready. They are expected to be present for assemblies and Personal Tutoring time. Pupils should return promptly after break and lunch and upload work onto *Teams* in a timely fashion. Pupils are expected to be fully engaged in all class activities. Failure to engage or produce work would result in the use of Reds on *Class Charts* in the first instance. Repeated failure to engage or to produce work would result in a parent meeting. Pupils must not use social media during online lessons.

Staff should ensure that they use *Teams* to communicate with pupils and not use other social media. They should keep a log of any behaviour incidents and report these in line with school procedures. Staff should teach with their camera on and blur the background if necessary. Teachers should have clear expectations about the use of microphones and supervise break-out groups and *Teams* chat to ensure high expectations of behaviour are maintained.