E-SAFETY POLICY

(INCLUSIVE OF CYBER BULLYING, ACCEPTABLE USE AND SOCIAL MEDIA)

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, governors, 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, 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.).

Legislation and Guidance

- In designing this policy, the School has considered the “4Cs” outlined in KCSIE (content, contact, conduct and commerce) as the key areas of risk.

Availability:

This policy is available on the School website.

Monitoring and Review:

This policy will be subject to continuous monitoring, refinement and audit by the Headteacher.

The Proprietor undertakes a formal review of this policy for the purpose of monitoring and of the efficiency with which the related duties have been discharged, by no later than one year from the date shown below, or earlier if significant changes to the systems and arrangements take place, or if legislation, regulatory requirements or best practice guidelines so require. The key priorities from the review are incorporated into the School Development Plan on an annual basis.

Reviewed by:

M Jenkin

Michelle Jenkin (Headmistress)
Date: 1st September 2025

Kane Andrews (Proprietor)
Date: 1st September 2025

Related Documents:

- Safeguarding Policies
- Staff Code of Conduct
- Behaviour Policy
- Data Protection Policy and Privacy Notices
- PSHE / RSE Policy

CONTENTS

1. INTRODUCTION

As a school, it is our duty to ensure that every pupil in our 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 and how to deal with any infringements.

At our 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.

Whilst we do not permit children to bring to school their own mobile devices, save where this is to support and specific and agreed IEP, we do, however, recognise that many pupils will have unlimited and unrestricted access outside of school to the internet via the internet and 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. The improper use of mobile technology by pupils, in or out of school, will be dealt with under the School's Behaviour Policy and Safeguarding and Policy as is appropriate in the circumstances.

2. ROLES AND RESPONSIBILITIES IN RELATION TO ONLINE SAFETY

All staff, proprietors, steering group members 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 line with the Safeguarding Policy.

2. 1. The Proprietors

The Proprietors have overall leadership responsibility for safeguarding as outlined in the Safeguarding Policy. The Proprietors of the School are responsible for the approval of this policy and for reviewing its effectiveness at least annually.

The Proprietors 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 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. 2. The Senior Leadership Team

The Headmistress 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, she is 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.

2. 3. The Designated Safeguarding Lead (DSL)

The DSL takes the lead responsibility for Safeguarding at our 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 Headmistress Senior Leadership Team and ICT Co-ordinator to achieve this. As such, in line with the Safeguarding 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 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.

The DSL oversees day-to-day responsibilities relating to online. They will keep up to date on current online safety issues and guidance issued by relevant organisations, including the Department for Education (including KCSIE), ISI, the CEOP (Child Exploitation and Online Protection), Childnet International and the Local Safeguarding Children Procedures.

2. 4. IT Service Provider

The School's IT service provider has 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 and its data, and maintain content filters, ensuring that reliable reporting is provided to the DSL against any inappropriate usage.

2. 5. Teaching and support staff

All staff are required to read and abide by the terms of the Acceptable Use Policy before accessing the School's systems. As with all issues of safety, 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.

All staff must read and understand this E-Safety Policy and enforce it in accordance with direction from the DSL, Senior Leadership Team and ICT C0-ordinator as appropriate.

2. 6. Pupils

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

2. 7. Parents and carers

We believe that it is essential for parents to be fully involved with promoting online safety both within and outside school. We 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 us.

3. FILTERING AND MONITORING

In general:
Our School aims to provide a safe environment to learn and work, including when online. Filtering and monitoring are important parts of our 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 DSL oversees regular checks that the filtering and monitoring system are operating effectively – these checks are recorded along with any appropriate action. From time to time the Chair of Proprietors, the DSL and external IT service provide 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, but not limited to, the following: age-inappropriate content and social reporting. If there is a good educational reason why a particular website, application, or form of content should not be blocked the relevant member of teaching staff will contact the DSL for their consideration.

We 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 to be identified. In line with our Data Protection Policy and/or Privacy Notices, usage and activity is continually monitored by our Filtering and Monitoring systems and incidents are raised to the DSL, who will investigate, record and take any appropriate actions as may be necessary. Teaching staff should notify the DSL if they are teaching material which might generate unusual internet traffic activity.

3. 1. 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 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.

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 DSL if they believe that appropriate teaching materials are being blocked.

3. 2. Pupils:

Pupils must report any accidental access to materials of a violent or sexual nature or that are otherwise inappropriate to the teacher supervising at that time, or otherwise to the 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 our filtering system. If this causes problems for schoolwork, pupils should their teacher for assistance.

4. EDUCATION AND TRAINING

4. 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 policy.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following the E-Safety procedures.

All teaching staff receive regular information and training (at least annually) on online safety issues in the form of 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 Policy, if there is a safeguarding concern a report must be made by staff to the DSL as soon as possible if any incident relating to online safety occurs.

4. 2. Pupils: the teaching of online safety

Online safety guidance will be given to pupils on a regular basis. 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 and IT lessons. Educating pupils on the dangers of technologies that may be encountered outside school will also be carried out via PSHE / RSE, by presentations in assemblies, as well as informally when opportunities arise.

At age-appropriate levels, pupils are taught about their online safety responsibilities and to look after their own online safety. Pupils can report concerns to the DSL and any member of staff at the school.

Pupils are taught about respecting their own and other people's information and images (etc.) through discussion and classroom activities.

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 Safeguarding and Behaviour 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.

4. 3. Parents

We seek to work closely with parents and guardians in promoting a culture of online safety. We will contact parents if we have any concerns about pupils' behaviour in this area and likewise hope that parents will feel able to share any concerns with the School.

We recognise 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 when our ICT co-ordinator discussed online safety and the practical steps that parents can take to minimise the potential dangers to their children without curbing their natural enthusiasm and curiosity.

5. USE OF SCHOOL AND PERSONAL DEVICES

5. 1. 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 are referred to the BYOD Policy, staff code of conduct and IT Acceptable Use Policy for further guidance on the use of non-school-owned electronic devices for work purposes.

Staff at are permitted to bring in personal devices for their own use. They may use such devices only during breaktimes and lunchtimes, and in designated areas away from children.

Without the express permission of the Headmistress and/or DSL, staff are not permitted under any circumstances to use their personal devices when taking images, videos or other recording of any pupil. Where express permission has be granted for a specific purpose, any image/recordings must be uploaded to the School network and deleted from the personal device as soon as this has been done. Staff must not have any images, videos or other recording of any pupil stored on their personal devices. Please read this in conjunction with Safeguarding, Acceptable Use and Staff Code of Conduct policies.

5. 2. Pupils

Children are not permitted, except in conjunction with the requirements of an IEP, to bring personal devices to school. Where, for personal safety, a child has use of a mobile device during travel to and from school (and the School has been notified of this by the parents/carers), the device must be handed to the Headmistress or Deputy Headmistress at the start of the day and may be collected as they leave school. These requirements apply to phones and all devices that communicate over the internet, including smartwatches and other wearable technology.

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 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 the SENCO to agree how the School can appropriately support such use. The SE$NCO will then inform the pupil's teachers and other relevant members of staff about how the pupil will use the device at school. Where the use of pupil-owned tablets/devices is prescribed under an IEP, pupils are required to adhere to the Acceptable Use and BYOD Policy when using devices for schoolwork. In particular, this requires pupils to ensure that their use of devices for schoolwork complies with this policy and prohibits pupils from using devices for non-school related activities during the school day.

6. ONLINE COMMUNICATIONS

6. 1. 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 / 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. 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, should not be shared with parents/carers unless in an emergency or as means of communication during residential visits. Save in an emergency, staff not contact parent/carer using a personal telephone number, email address, or other messaging system nor should parents/ carers be added as social network 'friends' or similar.

Under no circumstances should staff share their Personal telephone numbers, email addresses, or other contact details with pupils or recent alumni. Staff should never contact pupils/recent alumni using a personal telephone number, email address, or other messaging system nor should parents/ carers be added as social network 'friends' or similar.

Staff must immediately report to the Headmistress] 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 Headmistress.

6. 2. Pupils

All pupils are issued with their own personal login and password, which they use to access the school devices and software. Each account has a school email address and password, which will only be provided to the children in circumstances where it may be necessary to provide remote learning and access to applications such as Microsoft Teams. 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.

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 DSL.

7. USE OF SOCIAL MEDIA

7. 1. Staff

We have a Social Media Policy, which all staff should adhere to.

7. 2. Pupils

The children in our school are all below the minimum age for legal use of social media platforms. Parents/carers are required to ensure compliance and to support children in thinking carefully before they post any information online or repost or endorse content created by other people on any other platform they may use. 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 vary seriously and incidents will be dealt with under the Behaviour, Safeguarding and Anti-Bullying policies as appropriate.

8. RADICALISATION AND THE USE OF SOCIAL MEDIA TO ENCOURAGE EXTREMISM

The Internet and the use of social media in particular has become a major way to communicate with others, especially young people, which has provided access for like-minded people to create an online community and confirm extreme beliefs, sharing extreme ideological views or advocating the use of violence to solve problems. This has led to social media becoming a platform for:

- intensifying and accelerating the radicalisation of young people;
- confirming extreme beliefs;
- accessing likeminded people where they are not able to do this off-line, creating an online commnity;
- normalising abnormal views and behaviours, such as extreme ideological views or the use of violence to solve problems and address grievances.

St John's Priory School has a number of measures in place to help prevent the use of social media for this purpose:

- website filtering and monitoring is in place to help prevent access to terrorist and extremist material and social networking sites such as Facebook, Instagram or Twitter by pupils.
- pupils, parents and staff are educated in safe use of social media and the risks posed by on-line activity, including from extremist and terrorist groups.

We will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. The School cannot accept liability for any material accessed, or any consequences of internet access.

9. CYBERBULLYING

The use of ICT, particularly mobile electronic devices and the Internet, deliberately to upset someone else is known as Cyberbullying. Cyberbullying (along with all forms of bullying) will not be tolerated, and incidents of cyberbullying should be reported and will be dealt with in accordance with the School's Anti-Bullying Policy. Use of electronic devices of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline. If there is a suggestion that a child is at risk of abuse or significant harm, the matter will be dealt with under the School's Safeguarding Policy.

10. DATA PROTECTION

Please refer to the Data Protection policy and the Acceptable Use Policies 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 their school laptop / PC or to the School's systems (e.g., OneDrive, Teams) or the central server.

Staff devices should be encrypted if any data or passwords are stored on them. 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 service provider.

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

10. 1. Password security

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

All members of staff should:

- use a strong password, which should be changed regularly;
- not write passwords down; and
- not share passwords with pupils or other staff.

11. 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).

12. ARTIFICIAL INTELLIGENCE

As a school, we do not permit any usage by pupils of generative AI tools such as ChatGPT, Gemini, etc.

Where staff make use of generative AI tools, they must ensure that this is in adherence to other E-Safety policies, Acceptable Usage agreements, and subject to any conditions imposed. 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 and should not be relied on for accuracy.

We 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.

13. MISUSE

The 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 DSL. The DSL then may seek assistance from the CEOP, the LADO, and/or its professional advisers as appropriate.

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 Behaviour policies.

14. COMPLAINTS

As with all issues of safety at our school, if a member of staff, a pupil or a parent / carer has a complaint or concern relating to online safety prompt action will be taken to deal with it. Complaints should be addressed to the DSL in the first instance, who will liaise with the Senior Leadership Team and undertake an investigation where appropriate. Please see the Complaints Policy for further information.

Incidents of, or concerns around online safety will be recorded in accordance with the Safeguarding Policy and reported to DSL, in accordance with the School's Safeguarding Policy.

APPENDIX A – PUPIL ACCEPTABLE USE POLICY

All pupils must follow the rules outlined in this policy when accessing the school internet and systems, both in and outside of school, whether on school provided or personal devices. Breaking these rules may lead to behaviour sanctions and even, in some cases, criminal prosecution.

Pupil Declaration

I will:

- always use the School's ICT systems and the internet responsibly and for educational purposes only;
- only use them when a teacher is present, or with a teacher's permission;
- take care of school-issued devices;
- keep my usernames and passwords safe and not share these with others;
- keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer;
- tell a teacher (or trusted adult) immediately if I find any material which might upset, distress or harm me or others;
- always log off or shut down a computer when I've finished working on it; and
- if the School has approved for me to bring a personal device into school, I will sign it into the School Office before the start of the school day.

I will not:

- access any inappropriate websites including social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity;
- open any attachments in emails, or follow any links in emails, without first checking with a teacher;
- use any inappropriate language when communicating online, including in game chats;
- create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate;
- log in to the School's network using someone else's details; and
- arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision.

I agree to follow the school rules on the use of school network resources and ICT devices. I will use the network and all electronic devices in a responsible way and observe all of the conditions explained in this Acceptable Use Policy. I agree that the School will monitor the websites I visit. I understand that there will be consequences if I don't follow the rules.

Pupil's name ____

Pupil's Signature____________________________________ Date_________________

S	**Safe:** keep safe by being careful not to give out personal information – such as your full name, email address, phone number, home address, photos or school name – to people you are chatting with online
M	**Meeting:** Meeting someone you have only been in touch with online can be dangerous. Only meet people if you have your parents; or carers; permission and even then, only when they can be present
A	**Accepting:** Accepting emails, messages or invitations, or opening files, pictures or text from people you don't know could lead to problems and they may contain viruses or nasty messages.
R	**Reliable:** Information you find on the Internet may not be true, or someone online may be lying about who they are. Make sure you check information before you believe it.
T	**Tell:** Tell your parents, Kara or other trusted adults if somebody or something makes you feel uncomfortable or worried or if someone you know is being bullied online.

Parent/Carer agreement:

I understand that my child has agreed to accept the terms of the AUP Policy and I confirm that I accept the terms of the agreement. I acknowledge:

- Pupil access to networked resources is a privilege, not a right. Pupils will be expected to use the resources for the educational purposes for which they are provided. It is not possible to compile a complete set of rules about what is, and what is not, acceptable; however, the above should be a guide and in cases of dispute the decision of the Headmistress will be final.
- Pupils are also expected to use school resources in a responsible manner and any damage to them may result in fines to replace or fix damaged devices.
- Misuse of the internet will be dealt with in accordance with the School's Behaviour Policy and, where there is a safeguarding risk, the Safeguarding Policy.
- The School is not responsible for any loss of data on the network, computers connected to the network or data storage used on the network.
- Use of any information obtained via the network is at the pupil's own risk.
- If my child brings any personal devices to school, I understand that they are responsible for its safekeeping and appropriate usage while in transit to and from and at school.

I have read and understood the E-Safety Policy and agree to check any updates as the School provides.

Parent's name ____

Parent's Signature ______________________________ Date ______________

APPENDIX B: STAFF ACCEPTABLE USE POLICY

As a member of the school community I will follow these principles in all of my online activities:
I accept that the School cannot guarantee the confidentiality of content created, shared and exchanged via school systems.

I will:

- not access, create or share content that is illegal, deceptive, or likely to offend or misinform other members of the school community (for example, content that is obscene, or promotes violence, discrimination, conspiracy theories or extremism, or raises safeguarding issues);
- ensure that my online communications, and any content I share online, are respectful of others and composed in a way I would wish to stand by;
- respect the privacy of others. I will not share photos, videos, contact details, or other information about members of the school community, even if the content is not shared publicly, without going through official channels and obtaining permission;
- not access or share material that infringes copyright, and do not claim the work of others as my own;
- not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities; and
- not use my personal email, or social media accounts to contact pupils or parents.

Using the School's IT systems

Whenever I use the School's IT systems (including by connecting my own device to the network) I will follow these principles. I will:

- only access school IT systems using my own username and password. I will not share my username or password with anyone else;
- will not attempt by any means (including by the use of a Virtual Private Network (VPN)) to circumvent the content filters or other security measures installed on the School's IT systems, and will not attempt to access parts of the system that I do not have permission to access;
- will not attempt to install software on, or otherwise alter, school IT systems; and
- will not use the School's IT systems in a way that breaches the principles of online behaviour set out above.

I acknowledge that the School monitors use of the School's IT systems, and that the school can view content accessed or sent via its systems.

Passwords

Passwords protect the School’s network and computer system and are your responsibility. They should not be obvious (for example "password", 123456, a family name or birthdays), and nor should they be the same as your widely-used personal passwords. You should not let anyone else know your password, nor keep a list of passwords where they may be accessed and must change it immediately if it appears to be compromised. You should not attempt to gain unauthorised access to anyone else’s computer or to confidential information to which you do not have access rights.

Use of property

Any property belonging to the School should be treated with respect and care and used only in accordance with any training and policies provided. You must report any faults or breakages without delay.

Use of school systems

The provision of school email accounts, Wi-Fi and internet access is for official school business, administration and education. Staff should keep their personal, family and social lives separate from their school IT use and limit as far as possible any personal use of these accounts. Again, please be aware of the school's right to monitor and access web history and email use.

Use of personal devices or accounts and working remotely

All official school business of staff must be conducted on school systems, and it is not permissible to use personal email accounts for school business. Any use of personal devices for school purposes, and any removal of personal data or confidential information from school systems – by any means including email, printing, file transfer, cloud or (encrypted) memory stick – must be registered and approved by the Headmistress. Where permission is given for use of personal devices, these must be subject to appropriate safeguards in line with the School's policies, including [two-factor authentication, encryption etc.

Monitoring and access

Staff should be aware that school email and internet usage (including through school Wi-Fi) will be monitored for safeguarding, conduct and performance purposes, and both web history and school email accounts may be accessed by the school where necessary for a lawful purpose – including serious conduct or welfare concerns, extremism and the protection of others.

The School may require staff to conduct searches of their personal accounts or devices if they were used for school business in contravention of this policy, and in particular if there is any reason to suspect illegal activity or any risk to the wellbeing of any person.

Tracking devices and technology

The school is not responsible for individual settings on personal devices, nor for the use of tracking apps / devices for purely personal and domestic purposes.

Compliance with related school policies

To the extent they are applicable to you, you will ensure that you comply with the School's E- Safety Policy, and other relevant policies, including Retention of Records, Safeguarding and Data Protection Policy.

Retention of digital data

All emails sent or received on school systems should be deleted after 2-3 years and email accounts will generally be closed and the contents archived within 1 year of staff leaving the School.

Any information from email folders that is necessary for the School to keep for longer, including personal information (e.g. for a reason set out in the School privacy notice), should be held on the relevant personnel or pupil file. Important records should not be kept in personal email folders, archives or inboxes, nor in local files. Hence it is the responsibility of each account user to ensure that information is retained in the right place or, where applicable, provided to the right colleague. That way no important information should ever be lost as a result of the School's email deletion protocol.

Breach reporting

The law requires the School to notify personal data breaches, if they are likely to cause harm, to the authorities and, in some cases, to those affected. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This will include almost any loss of, or compromise to, personal data held by the school regardless of whether the personal data falls into a third party's hands. This would include:

- loss of an unencrypted laptop, USB stick or a physical file containing personal data;
- any external hacking of the School's systems, eg through the use of malware;
- application of the wrong privacy settings to online systems;
- misdirected post, fax or email;
- failing to bcc recipients of a mass email; and
- unsecure disposal.

The School must generally report personal data breaches to the ICO without undue delay (ie within 72 hours), and certainly if it presents a risk to individuals. In addition, controllers must notify individuals affected if that risk is high. In any event, the school must keep a record of any personal data breaches, regardless of whether we need to notify the ICO.

If either staff become aware of a suspected breach, you should notify the Data Compliance Lead.

Data breaches will happen to all organisations, but the School must take steps to ensure they are as rare and limited as possible and that, when they do happen, the worst effects are contained and mitigated. This requires the involvement and support of all staff. The School's primary interest and responsibility is in protecting potential victims and having visibility of how effective its policies and training are. Accordingly, falling victim to a data breach, either by human error or malicious attack, will not always be the result of a serious conduct issue or breach of policy; but failure to report a breach will be a disciplinary offence.

Breaches of this policy

A deliberate breach of this policy by staff will be dealt with as a disciplinary matter using the School's usual applicable procedures. In addition, a deliberate breach by any person may result in the School restricting that person’s access to school IT systems.

If you become aware of a breach of this agreement or the E- Safety Policy, or you are concerned that a member of the school community is being harassed or harmed online you should report it to the Headmistress. Reports will be treated in confidence wherever possible.

Acceptance of this policy

I confirm that I understand and accept this acceptable use policy

Name ____

Signature ___________________________ Date _______________