MALVERN ST JAMES
Girls' School

E-Safety Policy
(including Acceptable Use of IT and the Internet for Pupils and Staff - AUP)

This policy is the responsibility of the Designated Safeguarding Lead together with the E-Safety Officer (who is the IT Manager) to review and update annually.

Scope of this Policy

This policy applies to all members of the school community, including staff, pupils, parents, contractors and visitors, who have access to and are users of the school IT systems. In addition, this policy covers the use of personal digital devices accessing 3G r, 4G and/or 5G while on school premises. In this policy 'staff' includes teaching and operations staff, governors, and regular volunteers. 'Parents' includes pupils' carers and guardians. 'Visitors' include occasional volunteers but excludes any other ad-hoc visitors.

Both this policy and the Acceptable Use Policy (for all staff, visitors and pupils) cover fixed and mobile internet devices provided by the school (such as PCs, laptops, tablets, whiteboards, digital video equipment, etc.); as well as all devices owned by pupils, staff, contractors or visitors and used to access the School's IT systems (personal laptops, tablets, smart phones, etc.).

Introduction

It is the duty of Malvern St James (MSJ) Girls' School [hereafter 'the School'] to ensure that every pupil in its care is safe; the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose greater and more subtle 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 identity theft, bullying, harassment, grooming, stalking, abuse and radicalisation.

New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. Current and emerging technologies used in and outside of school include:

- Websites;
- Email and instant messaging;
- AI – Artificial Intelligence;
- Blogs;
- Social networking sites;
- Chat rooms;
- Music / video downloads;
- Gaming sites;
- Text messaging and picture messaging;
- Video calls;
- Podcasting;
- Online communities via games consoles;
- Mobile internet devices such as smart phones and tablets; and
- Use of Bluetooth technology.

Whilst exciting and beneficial both in and out of the context of education, much IT, particularly online resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies, which can be categorised as follows:

- **Content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
- **Contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **Conduct:** online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
- **Commerce:** - risks such as online gambling, inappropriate advertising, phishing and or financial scams.

At School we understand the responsibility to educate our pupils on e-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 e-safety and listening to their fears and anxieties as well as their thoughts and ideas.

This policy, supported by the Digital Device policy (for all staff, visitors, contractors 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.

This policy should be read and applied (where relevant) in conjunction with the following school policies, which are available via the School website and/or the Staff Handbook on the Shared Staff Resources Team.

- Safeguarding (including Child Protection) Policy
- Anti-Bullying Policy
- Photographic Images of Children Policy
- Data Protection Policy
- Whistleblowing Policy
- Complaints Policy
- Rewards and Sanctions Policy including Code of Conduct
- Policy for the use of Digital Devices.

Roles and Responsibilities

1. The Headmistress and the Senior Leadership Team

The Headmistress is responsible for the safety of the members of the school community and this includes responsibility for e-safety. The Headmistress has delegated day-to-day responsibility for e-safety to the Director of Pastoral Care (DoPC), who is also the Designated Safeguarding Lead (DSL), supported by the E-Safety Officer.

In particular, the role of the Headmistress and Senior Leadership Team (SLT) is to ensure that:

All staff, and in particular the Director of Pastoral Care (DSL) and the E-Safety Officer, are trained about e-safety as part of the wider safeguarding training (Appendix 1) and Staff are aware of the school procedures and policies that should be followed in the event of the abuse or suspected breach of e-safety in connection to the school. (Appendix 3).

2. The Director of Pastoral Care (DSL)

The Director of Pastoral Care (DSL) is accountable to the Headmistress for the day-to-day issues relating to e-safety and has responsibility for ensuring that this policy is upheld by all members of the school community, working with IT staff to achieve this. Safeguarding training and online safety training go hand in hand.

Supported by the E-Safety Officer and other subject matter experts drawn from across the School, the DoPC (DSL) will keep up-to-date on current e-safety issues and guidance issued by relevant organisations, including the Independent Schools Inspectorate, the Local Authority, CEOP (Child Exploitation and Online Protection), Childnet International and the Local Authority Safeguarding Children Board.

3. The E-Safety Officer

The E-Safety Officer is expected to keep up-to-date on E-safety issues and oversee delivery of E-safety education within MSJ in conjunction with the Director of Pastoral Care (DSL). The E-Safety Officer will be the principal advisor to the Safeguarding team on E-safety issues.

4. IT Support

The Director of Operations and Compliance ensures the School's technical staff have a key role in maintaining a safe technical infrastructure, training all staff that have access to the School IT system, monitoring data traffic (which includes filtering), and that they keep abreast with the rapid succession of technical developments. Additionally, the IT Dept will generate inappropriate usage reports to the DoPC (DSL) as required.

5. Staff

All members of the School community who have a school network logon are required to sign the Acceptable Use Policy (Appendix 3) and be familiar with the Digital Device policy before accessing the school's IT systems.

As with all issues of safety at MSJ, staff are encouraged to create a talking and listening culture in order to address any E-safety issues which may arise in classrooms on a daily basis.

6. Pupils

Pupils are responsible for using the school's IT systems in accordance with the Acceptable Use Policy (Appendix 3) and adhering to the Digital Device policy. Pupils must inform a member of staff if they see IT systems or digital devices being misused.

7. Parents and carers

The School believes that it is essential for parents to be fully involved with promoting E-safety both in and outside of school. The School will provide opportunities to consult and discuss E-safety with parents and will seek to promote a wide understanding of the benefits and risks related to internet usage. The School will always contact parents if there are any concerns about a pupil's behaviour in this area and it is expected that parents will feel able to share any concerns with the school.

Parents and carers are responsible for understanding and helping enforce the school's E-Safety and Digital Device policies.

Policy Statements

1. Use of School and 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. Staff should only use, the school device which is allocated to them, for school work. When they are not using a device, staff should ensure that it is locked to prevent unauthorised access.

Staff are permitted to bring in personal devices for their own use. They may only use such devices phones and tablets for teaching if a school device is not available. All personal devices must be protected with reputable antivirus software and operating systems and applications must be kept up-to-date.

Personal telephone numbers, email addresses, or other contact details should not be shared with pupils or parents/carers. Where possible, Staff must avoid contacting a pupil or parent/carer using a personal telephone number, email address, social media, or other messaging system.

Pupils

Unless required for specific classes, boarders should leave all personal portable devices in their respective Houses during the school day.

For pupils' use of personal devices, please refer to the Digital Device Policy, which is available via the relevant Team.

School mobile technologies available for pupil use (e.g. laptops) are to be securely stored in a departmental area. Access to these devices is only available through members of staff who should assign devices out and in before and after each use by pupils.

The School recognises that digital devices are now part of the day-to-day BYOD (Bring Your Own Device) learning environment. All members of the school community must adhere to the AUP. Pupils must have prior staff permission to use their personal devices.

2. Use of internet and email

Staff

Staff must not access social networking sites, online shopping or any website or personal email which is unconnected with school work or business from school devices or whilst teaching / in front of pupils. Such access may only be made from staff members' own devices away from pupils. School email addresses must not be used to subscribe to services that are not connected to school work/business.

When accessed from staff members' own devices/off school premises, 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.

The School has taken all reasonable steps to ensure that the school network is safe and secure. Staff should be aware that email communications through the school network and staff email addresses are monitored.

Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to IT Support. If in receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature, staff must immediately report to the E-Safety Officer or if unavailable, the DoPC. Staff must not respond to any such communication.

Any online communications by staff must neither knowingly or recklessly:

- place a child or young person at risk of harm, or cause actual harm;
- bring Malvern St James 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.

Under no circumstances should pupils be added as social network 'friends' or contacted through personal social media accounts. Each member of staff is responsible for ensuring high privacy settings across their personal social media accounts.

Any digital communication between staff and pupils or parents/carers must be professional in tone and content. Staff should not contact a pupil or parent/carer using any personal email address without first declaring such communications to the Designated Safeguarding Lead. The School ensures that staff have access to their work email address when offsite for use as necessary on school business. Staff are made aware that email communications through the school network and school email addresses are monitored, as they are the property of the School. Volunteers within the school are permitted access to emails, however wider access will be restricted.

Staff are encouraged to use the school's MIS to email parents and guardians.

Pupils

All pupils are issued with their own personal school email addresses for use on our network and by remote access. This will contain the word 'Pupil' in the descriptor to prevent information spillage by members of staff. Access is via a personal login, which is password protected. This official email service along with Teams, may be regarded as safe and secure, and must be used for accessing all school work, assignments / research / projects. Pupils are made aware that email communications through the school network and school email addresses are monitored as they are the property of the school.

There is strong anti-virus and firewall protection on our network and therefore spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for school work/research purposes, pupils should contact IT Support 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 the DoPC (DSL), E-Safety Officer, IT Support or another member of staff.

The School expects pupils to think carefully before they post any information online, or repost or endorse content created by other people. Content posted should not be able to be deemed inappropriate or offensive, or likely to cause embarrassment to the individual or others.

Pupils must report any accidental access to materials of a violent or sexual nature directly to the DoPC (DSL), E-Safety Officer, IT Support or another member of staff. Deliberate access to any inappropriate materials by a pupil will lead to the incident being recorded on their file and will be dealt with under the school's Behaviour Management Policy. Pupils should be aware that all internet usage via the school's systems and its Wi-Fi network is monitored.

3. Data storage and processing

The School takes its compliance with the UK General Data Protection Regulation (UK GDPR), which has consolidated and amended the Data Protection Act 2018 (DPA 2018) and the General Data

Protection Regulations seriously. Please refer to the school's Privacy Policy, the Acceptable Use Policy and Data Protection Policy for further details. Staff and pupils are expected to save all data relating to their work to their Microsoft OneDrive.

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 portable storage devices, such as memory sticks. Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the Director of Operations and Compliance via the online form available in the Shared Staff Resources Team.

4. Password security

Pupils and staff have individual school accounts and are regularly reminded of the need for password security. All pupils and members of staff must ensure that they do not write passwords down or share passwords with other pupils or staff. It is important for all members of the school community to create a strong password or passphrase (usually containing eight characters or more, and containing upper and lower case letters as well as numbers and symbols), and are prompted to change this should a data breach or risk occur.

5. 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 images on the internet (e.g. on social networking sites).

Parents/carers may not take videos and digital images of their children at school events, unless expressly permitted to do so in accordance with the Photographic Images of Children Policy. To respect everyone's privacy and in some cases protection, any images taken should not be published on blogs or social networking sites (etc.) without the permission of the people identifiable in them (or the permission of their parents), nor should parents comment on any activities involving other pupils in the digital / video images.

Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow this policy (including AUP) together with the Photography and Filming Policy concerning the sharing, distribution and publication of those images. Those images should, wherever possible, be taken on school equipment. If personal equipment is used, this should first be discussed with the DSL for permission; any images taken should be uploaded straight away on to the school network and deleted immediately from the personal device.

Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the School into disrepute.

Pupils may only take, use, share, publish or distribute images of others if it is line with the Photography and Filming Policy.

Written permission from parents or carers will be obtained before photographs of pupils are published on the school website (see Parent Contract/Acceptable Use Policy for more information). The School Office will ensure staff are aware of whose photos may not be used.

Photographs that include pupils and are published on the school website, or displayed elsewhere, will be selected carefully and will comply with good practice guidance on the use of such images. Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

6. Misuse

The School will not tolerate illegal activities or activities that are inappropriate in a school context, and will report illegal activity to the police and/or the Worcestershire LSCB (Local Safeguarding Children's Board). If the School discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from the CEOP (Child Exploitation and Online Protection).

Incidents of misuse or suspected misuse must be dealt with by staff in accordance with the school's policies and procedures (in particular the Safeguarding Policy). Appendix 3 provides a flowchart for dealing with an e-safety process incident.

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 Anti-Bullying Policy.

7. Education and Training

Details of the education and training requirements for staff, pupils and parents are outlined at Appendix 1.

8. Complaints and Concerns

As with all issues of safety at MSJ, if a member of staff, a pupil or a parent/carer has a complaint or concern, they should refer to the Complaints Policy for further information.

Incidents of/concerns around E-safety will be recorded using CPOMS and the Designated Safeguarding Lead will act in accordance with the school's Child Protection Policy.

Authorised by	Resolution of the School Council
Signature	
Date	21 June 2023

Effective date of the Policy	21 June 2023
Review date	Summer Term 2024
Circulation	Members of School Council / teaching staff / all staff / parents / pupils [on request]

Appendix 1

Education and Training

1. Staff: Awareness and Training

All new staff will receive information on the school's Safeguarding, E-Safety, including Acceptable Use and Digital Device policies as part of their induction and will be required to sign to confirm that they accept and understand the procedures therein. Staff are required to read and re-sign the AUP on annual basis.

All staff are to receive information and training on e-safety issues in the form of INSET training and internal meeting time. They are to be made aware of their individual responsibilities relating to the safeguarding of children within the context of e-safety. All supply staff must also receive information about e-safety as part of their safeguarding briefing on arrival at school.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school e-safety procedures. These behaviours are summarised in the Acceptable Use Policy which must be signed and returned before use of technologies in school. When children use school computers, staff should make sure children are fully aware of the agreement they are making to follow the school's IT guidelines.

Teaching staff are encouraged to incorporate e-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.

A record of concern must be completed by staff as soon as possible if any incident relating to e-safety occurs and be provided directly to the Designated Safeguarding Lead and Director of Pastoral Care on CPOMs

2. Pupils: e-Safety in the curriculum

IT and online resources are used increasingly across the curriculum. The School believes it is essential for e-safety guidance to be given to pupils on a regular and meaningful basis. We continually look for new opportunities to promote e-safety and regularly monitor and assess our pupils' understanding of it.

The School provides opportunities to teach about e-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 PSHEEC, by presentations in assemblies, as well as informally when opportunities arise.

Pupils are taught about their e-safety responsibilities and to look after their own online safety. In a graduated and age appropriate manner, the 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 the E-Safety Officer, Designated Safeguarding Lead, the Director of Pastoral Care or any member of staff at the School.

In a graduated and age appropriate manner, the pupils are taught laws applicable to using the internet; such as data protection and intellectual property. Pupils are taught about respecting 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 school's Anti-Bullying Policy, which describes the preventative measures and the procedures that will be followed when the school discovers cases of bullying). Pupils should approach the Designated Safeguarding Lead, Director of Pastoral Care, the E-Safety Officer or another

member of staff as well as parents and peers 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 e-safety. The School will always 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 digital devices at home. The School therefore arranges discussion evenings for parents about e-safety and the practical steps that parents can take to minimise the potential dangers to their child without curbing their natural enthusiasm and curiosity.

MALVERN ST JAMES
Girls' School

Acceptable Use of IT and the Internet for Pupils and Staff Policy

This policy is the responsibility of the Deputy Head, the Director of Operations and Compliance and the Director of Pastoral Care (DSL) to review and update annually.

Scope of this Policy

This policy applies to all members of the school community, including Staff, pupils, parents,contractors and visitors. In this policy, 'staff' includes teaching and Operations staff, Governors and regular volunteers. This policy should be read in conjunction with the following:

- Safeguarding (including Child Protection) Policy
- Staff Behaviour and Code of Conduct
- Anti-Bullying Policy
- Photography and Filming Policy
- Data Protection Policy
- Whistleblowing Policy
- Complaints Policy
- Rewards and Sanctions Policy (including Code of Conduct)
- Digital Devices Policy.

Malvern St James Computer Network and the Internet

The computer network is owned by Malvern St James and is made available to pupils to further their education, and to Staff to facilitate their roles. It is to support and enhance teaching and learning, as well as for carrying out the business of the School. Access to the Internet is provided through a filtered education provider for the safety of all users.

All members of the MSJ community must sign an Acceptable Use of IT and the Internet Agreement when they join MSJ and thereafter at the start of every academic year.

Members of Staff

All members of staff must sign an Agreement in terms of Appendix 3.

A reminder of the Acceptable Use Policy and an agreement request will appear on the staff member's screen once a term. The staff member will need to click "I Agree" before being able to continue accessing their account.

MALVERN ST JAMES
Girls' School

Acceptable Use of IT and the Internet Agreement for Pupils in Years 3 – 13

Any pupil wishing to use the Malvern St James Network and Internet access must agree to follow this Acceptable Use Policy (AUP). By signing this document, you are giving the School permission to monitor your usage of the School network, including emails.

The School reserves the right to examine or destroy any files that may be held on its computer system, including emails and to search and monitor any emails or Internet sites visited.

All Pupils will be required to access the Malvern St James network and Internet and, as such, must sign this copy of the Acceptable Use Policy and return it to MSJ Admissions prior to joining MSJ. Hereafter, each pupil will review and sign the AUP at the start of each academic year.

Pupils must only use their own account and must not share any login details with others. This will be dealt with as an equally serious offence as using another person's account.

Parents / Guardians are requested to endorse their child's signature.

As a School user of the Internet, I agree to follow the School rules on its use:

- I will abide by the School Code of Conduct and the Digital Device policy regarding the use of internet enabled devices, such as smart phones and iPads;
- I will use the network in a responsible way and observe all the restrictions explained to me by the School.;
- I will ensure my personal devices are protected with reputable antivirus software;
- I will ensure my personal device's operating system and applications are kept up-to-date;
- I give express consent for the monitoring and searching of my School account (my emails, internet usage and documents). My personal digital devices can be searched by a senior member of staff in my presence;
- I understand that breaking any of these rules may lead to stopping access to the Internet or computer network (or both). I also understand that misuse of technology, both inside and outside School, which affects the welfare of members of the School community or the reputation of the School will be subject to disciplinary procedures;
- I understand that the school owns the computer network and can set rules for its use. I understand it is a criminal offence to use a digital device or network for a purpose not permitted by the school;
- I will not do, write or publish anything using my personal digital device, such as a smart phone, iPad or laptop, that I would not be prepared to show to my parents, the Headmistress or a future employer;

- I will choose usernames that are appropriate and consider carefully what personal information I give out about my life, experiences and relationships;

- I will not be obscene either in the words I use or the content I view. This includes material that is racist, violent or adult in nature;

- I will not store or access inappropriate or illegal material;

- I will not send or post digital communications which are impolite, indecent, abusive, discriminatory, racist or in any way intended to make the recipient feel uncomfortable;

- I will respect the laws of copyright and ensure that sources used are referenced;

- I will not share content that puts me, or anyone else at risk in any way, this includes revealing passwords, personal details, photos or my location and will tell an adult should someone ask me for these details;

- I will not take or distribute any images, video or audio recordings of any staff or pupils without their consent;

- I will not upload or distribute digitally any image, video or audio content relating to the School or a Staff Member of the school community without permission from the Headmistress;

- I will never use my device to bully, physically threaten or upset anyone and will report any instances of bullying that I know about;

- I will report all instances of bullying on social media affecting any pupil at MSJ and I will recognise, even if I am not directly responsible for it, I have a duty to report it as I would be guilty by association;

- I understand that inappropriate use of the internet (including during holidays) may lead to disciplinary action in line with the Rewards and Sanctions policy;

- I will use my digital device as directed by my teachers and will do nothing to bring the school into disrepute;

- I will not send anonymous messages or chain mail;

- I will not attempt to circumvent the schools filtering in any way;

- I will not access or attempt to access unauthorised areas of the school network or any other computer network (this includes logging on to another user's account);

- I understand that torrenting, peer-to-peer networks or illegal file sharing are not permitted;

- I will acknowledge and adhere to the E-Safety rules;

- I understand that the school can check my computer files, emails and monitor the internet sites I visit.

Name of Pupil	
Pupil's Signature	
Date	

As the parent/guardian of the above-named pupil, I grant permission for my child to use electronic mail and the Internet in School. I understand that my child will be held accountable for their own actions.

Name of Parent/Guardian	
Parent/Guardian's Signature	
Date	

MALVERN ST JAMES
Girls' School

Acceptable Use of IT and the Internet Agreement for Pupils in EYFS and Years 1 & 2

Any pupil wishing to use the Malvern St James Network and Internet access must agree to follow this Acceptable Use Policy (AUP).

By signing this document, you are giving the School permission to monitor your child's usage of the School network, including emails.

The School reserves the right to examine or destroy any files that may be held on its computer system, including emails and to search and monitor any emails or Internet sites visited.

To ensure that all pupils understand the requirements of the AUP, regular time is allocated to the teaching of e-safety, including a dedicated lesson at the beginning of every term. In an age appropriate manner, all pupils are taught how to follow the Acceptable User Rules. They are reminded of the importance of keeping themselves safe on the Internet; how to follow the Internet Safety Rules; how to behave on the Internet and what to do when asked for personal information. Pupils are also made aware that, should they choose to break the Acceptable Use rules, they will be subject to age appropriate disciplinary procedures.

In Pre-Prep, Parents/Guardians are requested to sign the Acceptable Use Policy on behalf of their child.

Pupil's Full Name	
Year Group	

Your child will be expected to adhere to the following:

- I will use the network in a responsible way and observe all the restrictions explained to me by the School;
- I give express consent for the monitoring and searching of my School account (my emails, internet usage and documents). My internet-enabled and/or communication devices can be searched by a senior member of staff in my presence;
- I understand that breaking any of these rules may lead to stopping access to the Internet or computer network (or both). I also understand that misuse of technology, both inside and outside School, which affects the welfare of members of the School community or the reputation of the School, will be subject to disciplinary procedures.

As the parent/guardian of the above-named pupil, I grant permission for my child to use electronic mail and the Internet in School. I understand that my child will be held accountable for their own actions.

Name of Parent/Guardian	
Parent / Guardian's signature	
Date	

Please sign this document and return it to Admissions, admissions@malvernstjames.co.uk (new pupils) or Communications, communications@malvernstjames.co.uk (current pupils).

MALVERN ST JAMES
Girls' School

Acceptable Use of IT and the Internet Agreement for Staff

Any member of staff wishing to use the Malvern St James Network and Internet access must agree to follow this Acceptable Use Policy (AUP). By signing/confirming via Smartlog that you have read this document, you are giving the School permission to monitor your usage of the School network, including emails.

The School reserves the right to examine or destroy any files that may be held on its computer system, including emails and to search and monitor any emails or Internet sites visited.

Staff requesting Malvern St James Network and Internet access should sign this copy of the Acceptable Use Policy and return it to HR before starting at MSJ. Hereafter, staff will review and sign the AUP at the start of each academic year.

Staff must access the computer network only via their own account and password, which must not be available to any other person. Passwords should be strong and all users will be prompted to change these regularly.

Staff are responsible for the content of the emails they send. Emails must be formal and appropriate. Emails and messages sent to other forums accessed via the School network are School property and will be monitored. Posting anonymous messages and forwarding chain letters is forbidden.

If any pupil or member of staff is personally insulted, abused, libelled or bullied through the Internet or School network, this must immediately be reported to the Headmistress. Any abuse of the Internet or electronic device technology inside or outside School, which has a significant impact on School life, will also come under this Policy.

All activities that threaten the integrity of the School ICT systems or attack or corrupt other systems are forbidden. These include hacking, deliberate spreading of viruses, manipulating and deleting files other than their own and creating macros to the same end. Staff must respect the copyright of materials found on the Internet.

Staff must not use their mobile devices in the Pre-Prep(EYFS) Department.

When using the Internet or any social networking site (both during and following the termination of their employment) staff must not:

- post or publish any derogatory reference to the School, colleagues, parents or pupils;
- use commentary deemed to be defamatory, obscene, proprietary or libellous;
- discuss pupils or colleagues negatively or criticise the School or its staff; or
- misuse or inappropriately alter any text (written or audio), images or video clips featuring members of the School community.

Staff must respect the right of others to privacy and confidentiality. Text, images or clips of the School or members of the School staff can only be uploaded on School accounts on official School business in an appropriate manner and for no other purpose. Text, images or clips of pupils must not be uploaded to any internet site or distributed electronically without permission from the individual or their parent. This applies to both the School network and personal network. Please refer to the Photography and Filming Policy.

Staff must not attempt to avoid the filtering system in any way to gain access to restricted Internet sites. Staff must never use any network to access or spread inappropriate materials such as radicalising, pornographic, racist, sexually harassing or offensive text and images. Staff must never use School access to the Internet to pursue personal gain including online auctions, gambling, own political purposes/activism or advertising. Staff must immediately report to the Deputy Head, Director of Pastoral Care or E-safety Officer if they encounter undesirable material during any kind of communication on the Internet or computer network. Staff must not store inappropriate or illegal material.

The AUP also applies to staff who use their own laptops or any other Internet-enabled device. All devices must be password protected as a minimum and where possible encrypted. In addition, all laptops must have anti-virus software. It is the responsibility of each member of staff to keep this up-to-date and to ensure that all updates are installed. Laptops without anti-virus software will not be configured to access the school network or Internet.

Misuse of technology, both inside and outside of school, which affects the welfare of members of the school community or the reputation of the school will be subject to disciplinary procedures.

Staff must be aware that all files and emails sent or received on school systems are closed and the contents deleted within 3 months of them leaving the school. It is the responsibility of each account user to ensure that important information is retained in the right place or, where applicable, forwarded on to the appropriate colleague.

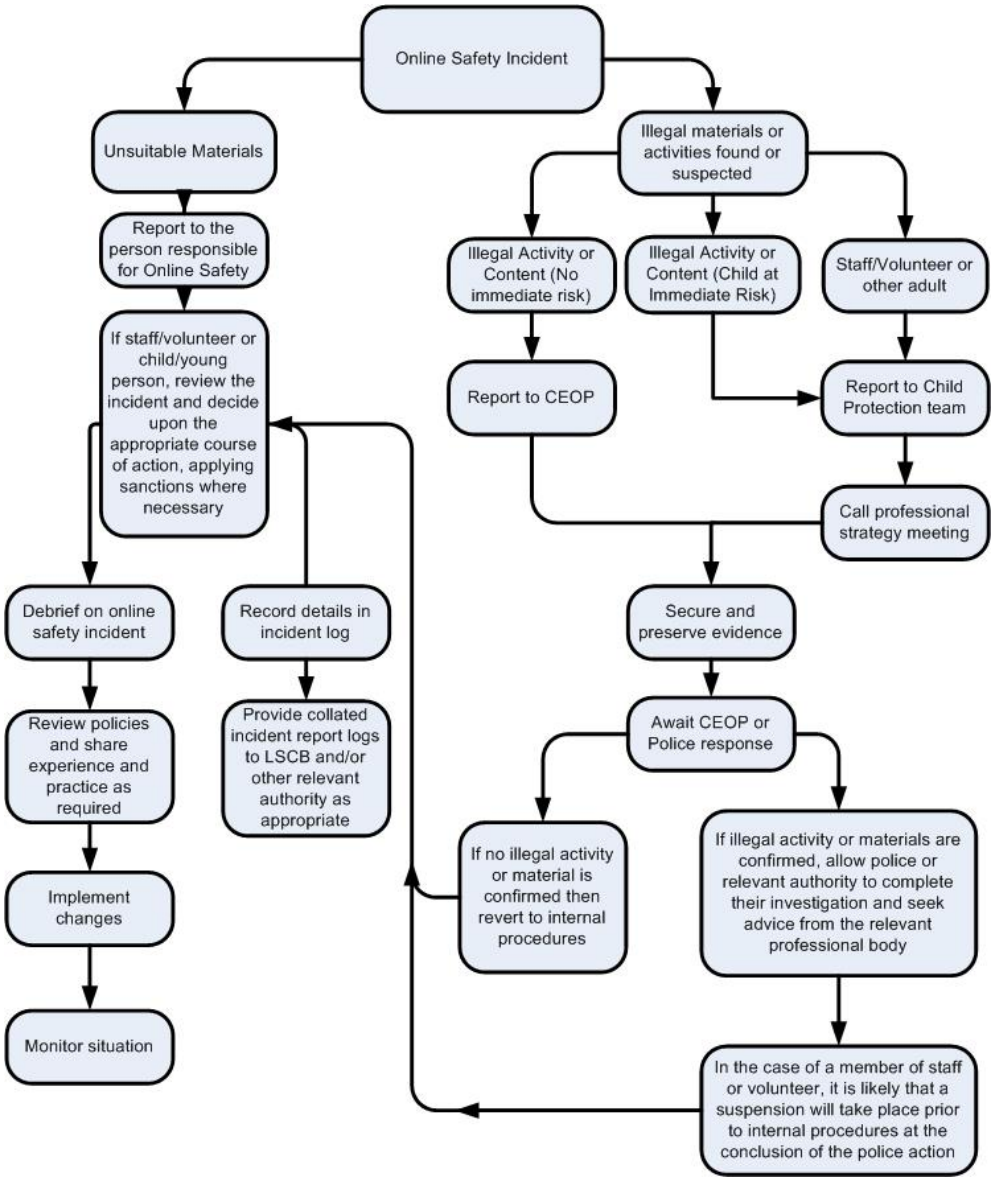
As a School user of the Internet, I agree to follow the School rules on its use:

- I will use the network in a responsible way and observe all the restrictions explained to me above;
- I give my express consent for the monitoring and searching of my School account (my emails, internet usage and documents);
- I will ensure my personal devices are protected with reputable antivirus software;
- I will ensure my personal device's operating system and applications are kept up to date;
- I understand that breaking any of these rules may lead to stopping access to the Internet or computer network (or both). I also understand that misuse of technology, both inside and outside School, which affects the welfare of members of the School community or the reputation of the School will be subject to disciplinary procedures.

Staff Full Name	
Department	
Staff Signature	
Date	

Appendix 3

Guidance on Responding to E-Safety Incidents of Misuse



Digital Do's & Don'ts

The MSJ AUP in plain English

All members of the MSJ Community must:

Behave appropriately online when using MSJ School Network or personal data

24 x 7 x 365
At ALL times

Have STRONG passwords!

Only use their own username & password

Have secure personal devices (2 level authentication)
& have up-to-date anti-virus software installed

Ensure that e mails are respectful & appropriate
NO chain letters permitted

Get permission for all PHOTOs, VIDEOs & AUDIO Recordings made on school property or on a school trip from staff member or trip leader

Get permission before SHARING or UPLOADING any TEXT, IMAGE or AUDIO Recording of the MSJ (includes property & uniform) or member of staff from the HEADMISTRESS

Get permission before SHARING or UPLOADING any material involving another MSJ pupil at ALL times & ALL places

NEVER use a VPN to access blocked areas of the MSJ Network

Only access AGE-APPROPRIATE apps and sites

ALWAYS be KIND & RESPECTFUL
Never Cyberbully

Never access or store INAPPROPRIATE Material (texts, images, files, recordings etc), this includes extremist views, sexually explicit, upsetting (violent and graphic) or offensive material.

ALLOW a member of senior staff to check personal devices in event of misuse of technology

NEVER bring MSJ into disrepute