MORE HOUSE SCHOOL

POLICY

SAFE USE OF TECHNOLOGY

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, governors, supply staff, contractors, volunteers, parents/carers and visitors) who have access to and are users of More House School's IT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers/Principals to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour for Learning Policy.

The school will deal with such incidents within this policy and associated behaviour for learning and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Policy Statement

The internet holds huge potential for children and young people. It is a fun and exciting place to explore and it helps children and young people to learn at home as well as in school. The internet and use of mobile devices are now a part of the daily social and educational lives of children and young people, and it is therefore vitally important that we are aware of the risks so that children and young people can make the most of the opportunities available to them while remaining safe.

All pupils, parents, staff, supply staff, contractors, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's IT facilities and systems. 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 House School aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology.
- Teach pupils how to stay safe in the digital world and how to manage their own behaviour to avoid making themselves vulnerable to a range of risks, including online grooming and sexual exploitation.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

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

Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education 2023, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Searching, screening and confiscation
- Prevent Duty Guidance
- Meeting digital and technology standards in schools and colleges

It also refers to the following guidance:

- DfE's guidance on protecting children from radicalisation.
- Education Act 1996 (as amended)
- Education and Inspections Act 2006
- Equality Act 2010
- Education Act 2011

Roles and responsibilities

The Board of Governors

The Board of Governors has overall responsibility for monitoring this policy and for reviewing the effectiveness of the policy.

MORE HOUSE SCHOOL

POLICY

SAFE USE OF TECHNOLOGY

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with the Head of IT Services and the DSL what needs to be done to support the school in meeting those standards, which include:

- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

All governors will:

- Ensure that they have read and understood this policy.
- Agree and adhere to the terms of acceptable use of the school's IT facilities and systems.
- Ensure that, where necessary, teaching about safeguarding, including online safety is adapted for vulnerable children and victims of abuse. Because the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.
- Regularly review the effectiveness of the schools filtering and monitoring systems.
- Make sure online safety is a running and interrelated theme within the whole school approach to safeguarding and related policies.
- Make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The Headmaster

- The Headmaster is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.
- The Headmaster has a duty of care for ensuring the safety (including online safety) of members of the school community, although the day-to-day responsibility for online safety will be delegated to the Designated Safeguarding Lead (DSL).
- The Headmaster and the DSL are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Headmaster is responsible for ensuring that the DSL and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

The Designated Safeguarding Lead

The DSL takes lead responsibility for online safety in the school, in particular:

- Lead responsibility for safeguarding and online safety, which could include overseeing and acting on:
    - filtering and monitoring reports
    - safeguarding concerns
    - checks to filtering and monitoring systems
- Supporting the Headmaster in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the Headmaster, Head of IT Services and other staff, as necessary, to address any online safety issues or incidents.
- Has the day-to-day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents.
- Managing all online safety issues and incidents in line with the school's Safeguarding and Child Protection policy.
- Ensuring that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged on CPOMS and dealt with appropriately in line with this policy.

- Receiving reports of online safety incidents and creating a log of incidents to inform future online safety developments.
- Undertaking annual risk assessments that consider and reflect the risks children face.
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively.
- Ensure staff receive relevant information about emerging issues.
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the Headmaster and Board of Governors.

This list is not intended to be exhaustive.

The Head of IT Services

The Head of IT Services is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- The filtering policy is applied and updated on a regular basis.
- Ensuring that the school's technical infrastructure is secure and is not open to misuse or malicious attack and is protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Keeping up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- The use of the school's IT facilities and systems are regularly monitored in order that any misuse/attempted misuse can be reported to the Headmaster and DSL for investigation/action/sanction.
- Conducting a full security check and monitoring the school's IT systems continuously.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Supplying the Senior Management Team regular monitoring reports.

This list is not intended to be exhaustive.

All staff and volunteers

All staff, including contractors and supply staff, and volunteers are responsible for:

- Maintaining an understanding of this policy.
- Implementing this policy consistently.
- Agreeing and adhering to the terms on acceptable use of the school's IT facilities and systems and ensuring that pupils follow the school's terms on acceptable use.
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents.
- Working with the DSL to ensure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy.
- Ensuring that any concerns relating to cyber-bullying, online grooming or the viewing of inappropriate material must be reported on CPOMS and dealt with appropriately in line with this policy.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'.
- Reinforce the importance of online safety when communicating with parents and carers. This includes making parents aware of what we ask children to do online (e.g. sites they need to visit or who they'll be interacting with online)

This list is not intended to be exhaustive.

Pupils

- Are responsible for using the school's IT facilities and systems in accordance with the pupil acceptable use policy.
- To have an understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand policies on the use of mobile devices. They should also know and understand policies on the taking/use of images and on online-bullying.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school.

Parents and carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. More House School will take every opportunity to help parents and carers understand these issues through newsletters, the school's website, social media and information about national/local online safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good online safety practice.

Parents are expected to:

- Ensure their child has read, understood and agreed to the terms on acceptable use of the IT facilities and systems.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International
- Healthy relationships – Disrespect Nobody

Visitors and members of the community

Visitors and members of the community who use the school's IT facilities and systems will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms of acceptable use.

Education and Training

Educating pupils about online safety

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety/digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Pupils will be taught about online safety as part of the PSHEE curriculum. The safe use of social media and the internet will also be covered in other subjects where relevant. Where necessary, teaching about safeguarding, including online safety will be adapted for vulnerable children and victims of abuse.

Educating parents and carers about online safety

Parents and carers may have a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will raise parents' and carers' awareness of online safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the DSL and/or the Headmaster.

Staff Training
All new staff members will receive training, as part of their induction, on online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff briefings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse.
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic/misandrist messages.
    - Non-consensual sharing of indecent, nude and semi-nude images and/or videos, especially around chat groups.
    - Sharing of abusive images and pornography, to those who don't want to receive such content.
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse.
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up.
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term.

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

More information about safeguarding training is set out in our Safeguarding and Child Protection policy.

Governors
Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Access and Security

Technical – infrastructure/equipment, filtering and monitoring
More House school will provide managed internet access to its staff and pupils. This will help pupils learn how to assess and manage risk, to gain the knowledge and understanding to keep themselves safe when using the internet and to bridge the gap between school IT systems and the more open systems outside school.

More House School will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety

responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by the IT department who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- The "master/administrator" passwords for the school systems, used by the Network Manager must also be available to the Headmaster or other nominated senior leader and kept in a secure place.
- The Head of IT Services is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content (e.g., child sexual abuse images) is filtered by Sonicwall by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly reviewed.
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The school has provided enhanced/differentiated user-level filtering.
- Systems are in place to ensure that internet use can be monitored, and a log of any incidents will be kept by the DSL to help to identify patterns of behaviour and to inform this policy.
- The activity of users on the school IT facilities and systems is regularly monitored and users are made aware of this in the acceptable use policy.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices, etc. from accidental or malicious attempts, which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual devices are protected by up to date anti malware software.
- The school will ensure that access to the internet via school equipment for everyone is filtered and monitored.

The school reserves the right to monitor the use of its IT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- User activity/access logs
- File Storage
- Database use
- Any other electronic communications

Only authorised SMT may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The school monitors IT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and IT operation

- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

Authorising access

- All staff (including supply staff, contractors and governors) must read and sign the relevant AUP (Acceptable Use Policy)' before accessing the school IT facilities and systems.
- The school will maintain a current record of all staff and pupils who are granted access to school IT facilities and systems.
- All pupils must apply for internet access individually by agreeing to comply with the pupil AUP.
- People not employed by the school must read and sign a Guest AUP before being given access to the internet via school equipment.

Remote access

We allow staff to access the school's IT facilities and materials remotely.

Staff accessing the school's IT facilities and systems remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the school's IT facilities outside the school and take such precautions as the Head of IT Services may require.

Our IT facilities and systems contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

Use of personal devices

Personal equipment may be used by staff and/or pupils to access the school IT facilities and systems provided their use complies with this policy and the relevant AUP below.

Staff must not store images of pupils or pupils personal data on personal devices.

More House School cannot be held responsible for the loss of, or damage to, any personal devices used in school or for school business.

Protecting personal data

More House School has a separate Data Protection Policy. It covers the access to pupil and staff personal data on and off site, and remote access to school systems.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit before use in school is allowed.
- More House School is aware that technologies such as mobile phones and smart watches with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communications.

Assessing risks

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

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 online-bullying 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. It is common for employers to carry out internet searches for information about potential and existing employees. More House School will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

- 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.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website/social media/local press.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers 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 school policies concerning the sharing, distribution and publication of those images. Other than in exceptional circumstances, staff must use equipment provided by the school for such purposes, and not use personal equipment.
- 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 must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils 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.
- Written permission will be obtained from parents or carers before photographs of pupils are published on the school website or any school run social media as set out in Surrey Safeguarding Children Board Guidance on using images of children. (http://www.surreycc.gov.uk/?a=168635)
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Further information is available in the Taking, storing and using Images of Children policy.

Online-safety rules

It is appropriate for people to be allowed a great deal of freedom in using IT for study, work and leisure. With freedom comes responsibility. More House School cannot control what people, all over the world, make available on the internet; a small proportion of the material which it is possible to access is not acceptable in school, whilst other material must be treated with great sensitivity and care. Exactly the same standards apply to electronic material, as to material in any other form.

We value all of our pupils equally. It is therefore part of the ethos of More House School to promote considerate behaviour and to value diversity both offline and online. The School is committed to promoting amongst its entire community respect for, and accordance with the fundamental British Values of democracy, the rule of law, individual liberty and mutual respect for and tolerance of those with different faiths and beliefs, and those without faith. Bullying and harassment in any form should always be reported to a member of staff. It is never the victim's fault, and they

should not be afraid to come forward.

Artificial Intelligence (AI)
Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

More House School recognises that AI has many uses to help pupils learn but may also have the potential to be used to bully and/or harm others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

More House School will treat any use of AI to bully/and or harm other pupils in line with our Behaviour for Learning policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

Community use of the internet
Members of the community and other organisations using the school internet connection will have signed a guest AUP so it is expected that their use will be in accordance with this policy.

Unacceptable and inappropriate use
The following is considered unacceptable use of the school's IT facilities and systems by any member of the school community. Any breach of this policy may result in disciplinary or behaviour proceedings or referral to contracting and/or external agency as appropriate.

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to **illegal** activity such as:
- Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978
- Child exploitation
- Child abuse
- Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003
- Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008
- Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986

Activities that might be classed as cyber-crime under the Computer Misuse Act:
- Gaining unauthorised access to school networks, data and files, through the use of computers/devices
- Creating or propagating computer viruses or other harmful files
- Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)
- Disable/impair/disrupt network functionality through the use of computers/devices
- Using penetration testing equipment (without relevant permission)

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:
- Threatening behaviour, including promotion of physical violence or mental harm.

- Violent or that glorifies violence or cruelty.
- Encouraging vandalism, suicide, self harm or eating disorders.
- Criminal, terrorist or glorified criminal activity (including drug abuse).
- Crude, profane or with otherwise unsuitable language.
- Blasphemous or mocking of religious and moral beliefs and values.
- Radicalised, extremist, of extreme political opinion, racist, inciting racial hatred, anti-Semitic or discriminatory in any other way.
- Pornographic, offensive, obscene or otherwise inappropriate or harmful.
- Using inappropriate or offensive language.
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth-produced sexual imagery).
- Online gambling, inappropriate advertising, phishing and/or financial scams.
- Breaching the school's policies or procedures.
- Activity which defames or disparages the school, or risks bringing the school into disrepute.
- Sharing confidential information about the school, its pupils, or other members of the school community.

Other unacceptable use:

- Using other people's user ID or password, even with their permission.
- Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school.
- Searching for or using websites or mechanisms to bypass the school's filtering mechanisms.
- Attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel.
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the school's IT facilities.
- Removing, deleting or disposing of IT equipment, systems, programs or information without permission by authorised personnel.
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation.
- Promoting a private business, unless that business is directly related to the school.
- Revealing any personal details including a home address or mobile telephone number to strangers.
- Using the school's IT facilities to bully or harass someone else, or to promote unlawful discrimination.
- Using the school's IT facilities to breach intellectual property rights or copyright.
- Causing intentional damage to IT facilities or materials.

This is not an exhaustive list. The School reserves the right to amend this list at any time. The Headmaster will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's IT facilities and systems.

In order to protect responsible users, electronic methods will be used to help prevent access to unsuitable material. More House School reserves the right to access all material stored on its IT systems, including that held in individual areas of staff and pupil accounts for purposes of ensuring DfE, Local Authority and school policies regarding appropriate use, data protection, computer misuse, child protection, and health and safety. Anyone who is found not to be acting responsibly in this way will be ~~disciplined~~ sanctioned.
More House School will act strongly against anyone whose use of IT risks bringing the school into disrepute or risks the proper work of other users.

Unacceptable use of IT and the internet outside of school - pupils

The School will sanction pupils, in line with the Behaviour for Learning policy if a pupil engages in any of the following at any time (even if they are not on school premises):

- Using IT or the internet to breach intellectual property rights or copyright.
- Using IT or the internet to bully or harass someone else, or to promote unlawful discrimination.
- Breaching the school's policies or procedures.
- Any illegal conduct, or statements which are deemed to be advocating illegal activity.
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate.
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery).
- Activity which defames or disparages the school, or risks bringing the school into disrepute.
- Sharing confidential information about the school, other pupils, or other members of the school community.
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's IT facilities.
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation.

Staff using the school's IT facilities outside school

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

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends, unless they have their own login details
- Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use.

If staff have any concerns over the security of their device, they must seek advice from the IT Services department.

Staff personal use of the school's IT facilities

Staff are permitted to occasionally use school IT facilities for personal use subject to certain conditions set out below. Personal use of IT facilities must not be overused or abused. The Headmaster may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during contact time/teaching hours/non-break time
- Does not constitute 'unacceptable use', as defined above
- Takes place when there are no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may not use the school's IT facilities to store personal non-work-related information or materials (such as music, videos or photos).

Staff should be aware that use of the school's IT facilities for personal use may put personal communications within the scope of the school's IT monitoring activities. Where breaches of this policy are found, disciplinary action may be taken.

Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with this policy.

Staff should be aware that personal use of IT (even when not using school IT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where pupils and parents could see them.

Staff should take care to follow the school's guidelines on social media and use of email to protect themselves online and avoid compromising their professional integrity.

Use of Email

The School provides each member of staff with an email address. This email account should be used for work purposes only and all work-related business should be conducted using only this email.

Staff must not share their personal email addresses with parents and pupils, and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error that contains the personal information of another person, they must inform the Bursar and Head of IT Services immediately who will follow our data breach procedure.

- Pupils and staff may only use approved e-mail accounts on the school IT systems
- Staff to pupil electronic communication must only take place via a school email address or from within Teams
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known
- The School will monitor how e-mail from pupils' school accounts to external bodies is presented and controlled

Published content (e.g., school website, school social media accounts)

- The contact details will be the school address, email and telephone number. Private information will not be published
- The Headmaster or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate

Social Media

All schools have a duty of care to provide a safe learning environment for pupils and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The School provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- The School will control access to social networking sites and consider how to educate pupils in their safe use. This control may not mean blocking every site; it may mean monitoring and educating pupils in their use.
- Staff and pupils should ensure that their online activity, both in school and out takes into account the feelings of others and is appropriate for their situation as a member of the school community.

- Ensuring that personal information is not published.
- Clear reporting guidance, including responsibilities, procedures and sanctions.

School staff should ensure that:

- No reference should be made in social media to pupils, parents/carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the School.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Communication and response

Communication of the Policy

To pupils:

- Pupils need to agree to comply with the pupil AUP in order to gain access to the school IT facilities and systems and to the internet.
- Pupils will be reminded about the contents of the AUP as part of their online-safety education.

To staff:

- All staff will be shown where to access this policy and its importance explained.
- All staff must sign and agree to comply with the staff AUP in order to gain access to the school IT facilities and systems.
- All staff will receive online-safety training on an annual basis.

To parents and carers:

- The School will ask all new parents and carers to sign the parent /pupil agreement when they register their child with the school.
- Parents' and carers' attention will be drawn to online safety in newsletters, and on the school website.

Handling online-safety complaints

Complaints of internet misuse will be dealt with in accordance with this policy.

Complaints of a child protection nature must be dealt with in accordance with the school's Safeguarding and Child Protection policy.

Pupils and parents will be informed of consequences and sanctions for pupils misusing the internet in accordance with the Behaviour for Learning policy.

Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, tablet devices, laptops and smart watches, where they believe there is a 'good reason' to do so.

It is up to the DSL, Headmaster or a member of the CLG to decide whether there is a good reason to carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

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

- Make an assessment of how urgent the search is and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from DSL or Headmaster.
- Explain to the pupil why their device is being searched, how the search will happen, and give them the opportunity to ask questions about it.
- Seek the pupil's co-operation.

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Break any of the school rules, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the DSL or other member of the safeguarding team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school ~~discipline~~ rules), 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 devices will be carried out in line with:
The DfE's latest guidance on screening, searching and confiscation and UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

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

How the school will respond to issues of misuse
Where a pupil misuses the school's IT facilities and systems, we will follow the procedures set out in our Behaviour for Learning policy. 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 IT facilities and systems 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.

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.

- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and kept for further investigation (except in the case of images of child sexual abuse – see below).
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or ~~discipline~~ sanction procedures
    - Involvement of the Local Authority
    - Police involvement and/or action
- If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - Incidents of 'grooming' behaviour
    - The sending of obscene materials to a child
    - Adult material which potentially breaches the Obscene Publications Act
    - Criminally racist material
    - Promotion of terrorism or extremism
    - Offences under the Computer Misuse Act
    - Other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

Acceptable Use of Mobile Devices Policy (inc BYOD)

Definition

For the purpose and interpretation of this policy, 'mobile devices' includes laptops, mobile phones, gaming consoles, ipods, tablets, smart watches and any other device that is capable of accessing the internet or transferring/receiving digital information.

Rationale

The absolute key to considering the use of mobile devices is that the pupils, staff and wider school community understand that the primary purpose of having their personal device at school is educational and that this is irrespective of whether the device is school owned/provided or personally owned. However, the school recognises that personal communication through mobile technologies is an accepted part of everyday life but that such technologies need to be used appropriately and safely.

This policy sits alongside the Safeguarding and Child Protection policy, Anti-bullying policy, Acceptable Use Policy, and the Behaviour for Learning policy.

Potential Benefits of Mobile Technologies

Research has highlighted the widespread uptake of mobile technologies amongst adults and children of all ages. Web-based tools and resources have changed the landscape of learning. Pupils now have at their fingertips unlimited access to digital content, resources, experts, databases and communities of interest. By effectively maximizing the use of such resources, schools not only have the opportunity to deepen student learning, but they can also develop digital literacy, fluency and citizenship in pupils that will prepare them for the high tech world in which they will live, learn and work.

Purpose

- The School recognizes the convenience of pupils using their own devices for educational purposes and this policy is intended to enable this to happen safely and positively.
- The widespread ownership of mobile and smart devices among young people requires that school administrators, teachers, pupils, parents and carers take steps to ensure that mobile and smart devices are used responsibly at school. This Acceptable Use of Mobile Devices policy is designed to ensure that potential issues involving mobile devices can be clearly identified and addressed, ensuring the benefits that mobile devices provide (such as increased safety) can continue to be enjoyed by our pupils.
- More House School has established the following Acceptable Use Policy for mobile devices that provides staff, pupils, parents and carers guidelines and instructions for the appropriate use of mobile devices during school hours.
- Staff, pupils, their parents or carers must read and understand the Acceptable Use Policy as a condition upon which permission is given to bring mobile devices to school.
- The Acceptable Use Policy for mobile devices also applies to pupils during school excursions, camps and extra-curricular activities both on the school campus and off-site.

General use of personally owned mobile devices

- Personally owned mobile devices brought in to school are the responsibility of the device owner. The School accepts no responsibility for the loss, theft or damage of personally owned mobile devices, irrespective of whether or not the pupil is using it as part of a lesson.
- Mobile and personal devices are not permitted to be used in certain areas within the school site such as changing rooms and toilets.
- Mobile devices will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with explicit consent from a member of staff.

- No images or videos should be taken on mobile devices without the prior consent of the person or people concerned.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for IT acceptable use as set out above. School phones should not be used for personal matters except in an emergency of exceptional circumstances.

Staff use of personally owned mobile devices

- Some members of staff will be issued with a school device where contact with pupils, parents or carers is required. Where staff members are required to use a mobile device for school duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents, then a school mobile device will be provided and used. In an emergency where the staff member doesn't have access to a school owned device, they should use their own devices and hide (by inputting 141 or blocking Caller ID) their own mobile numbers for confidentiality purposes.
- Personally-owned devices must be switched off or switched to 'silent' mode, Bluetooth communication should be 'hidden' or switched off and mobile devices must not be used during teaching periods unless permission has been granted by the Headmaster, or in emergency circumstances.
- Staff must not store photos or videos of pupils on their privately owned devices and will only use school provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken as appropriate.
- Staff use of mobile devices during the school day will normally be limited to non-contact times of the school day.
- Staff should ensure that their devices are protected with PIN/access codes in case of loss or theft.
- Staff should not send and read texts in classrooms or use camera devices at any time unless part of a teaching or learning process.
- Staff must not give their personal phone numbers to parents or pupils.
- If a member of staff needs to make telephone contact with a parent, a school telephone should be used.
- Staff should never store parents' or pupils' telephone or contact details on their mobile device, as this allows the possibility of inappropriate contact.
- Staff should never send, or accept from anyone, texts or images that could be viewed as inappropriate.
- If a member of staff suspects a message, text or similar may contain inappropriate content it should not be opened and the DSL should be contacted.

Pupils' use of personally owned mobile devices

For years 4-11:

Pupils may not access or switch on their mobile phone during the school day, between 8.30am and 4.20pm. If a pupil does bring in their phone it must remain in their bag and switched off at all times.

More House School – Mobile Phone Policy

1. Do you need your phone in school?

You are not permitted to use it during the school day, so please think carefully about whether it is worth bringing it in. If you do bring it in, you are welcome to leave it with your form tutor.

2. When you enter your form room, you will be asked to place your mobile phone, including AirPods or other accessories, into your bag. It is at this point that you can leave it with your tutor if you wish.

3. If you are seen with a mobile phone, AirPods or other accessories, you will be asked to surrender your device to the staff member who has requested it from you (to make clear, if you have AirPods in, you must have a mobile phone on you or nearby, and therefore you will be asked to hand in both devices).

4. Once your mobile device(s) has been surrendered, it will be delivered to your form tutor for a return at the end of the school day.
5. If you are requested, for a second time, to surrender your device, you will then meet with your Head of Year who will sign the device in and out at the start and end of each day until a plan has been put in place to avoid further use of the device(s).
6. If you refuse to hand your device(s) in, you will be referred to your Head of Year and/or the Director of Pastoral Care, who will determine the period by which the device(s) either remains at home, or the period the device is signed in and out at the start and end of each day. In exceptional circumstances, you may be requested to meet with the Deputy Head (Pastoral), to determine an approach moving forward.

If you need to call somebody during the school day, you should go to the main reception, and the office staff will help you to speak to the person you need.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement.

If a pupil breaches the school policy then the device will be confiscated and will be held in a secure place by their form tutor, but may be passed to senior staff members as necessary.

Parents are advised not to contact their child via their mobile device during the school day, but to contact the School Office.

Pupils should protect their device numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile devices and will be made aware of boundaries and consequences and encouraged to use PIN's and other security as necessary.

For 6th Form:
Pupils may bring mobile devices into school, they may be used during breaks, lunch times and at the end of the school day, after afternoon registration.

Use of personal devices on school grounds is at the discretion of school staff. All pupils MUST use their devices as directed by their teacher and staff.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement.

If a pupil breaches the school policy then the device will be confiscated and will be held in a secure place by their form tutor, but may be passed to senior staff members as necessary.

Devices must not be taken into examination rooms. Pupils found in possession of a mobile device during an examination will be reported to the appropriate examining body. This may result in the withdrawal of the pupil from either that examination or all examinations.

Parents are advised not to contact their child via their mobile device during the school day, but to contact the School Office.

Pupils should protect their device numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile devices and will be made aware of boundaries and consequences and encouraged to use PIN's and other security as necessary.

Responsibility

- It is the responsibility of pupils who bring mobile devices to school to abide by the guidelines outlined in this policy.
- The decision to provide a mobile device to their children should be made by parents/carers. It is incumbent upon parents/carers to understand the capabilities of the device and the potential misuse of those capabilities.
- Parents/carers should be aware that if their child takes a mobile device to school it is assumed household insurance will provide the required cover in the event of loss or damage. The School cannot accept responsibility for any loss, damage or costs incurred due to its use or misuse.
- It is the pupil's and parent or carer's responsibility to ensure that their personal device is kept up to date with the latest operating system updates and upgrades.
- It is the pupil's responsibility to ensure that their device is kept secure. Every pupil's personal device must be password protected. Additionally, the appropriate security software must be installed to protect personal devices against the latest malicious threats such as viruses, malware, etc.
- Parents/carers are recommended to have adequate insurance coverage in place to cover the cost of replacement or repair of the pupil's personal device in the event of loss or damage that occurs on school premises, or during school visits and activities.

Please note, the school is will not accept any liability for the following:

- Any personal mobile device that is broken on school premises or during school visits and outside activities.
- Any personal devices that are stolen or lost on school premises or during school visits and outside activities.
- Any personal data that is lost on personal devices while they are being used on school premises.

Acceptable Uses

- Pupils are only permitted to use mobile devices in classrooms with permission.
- Parents/carers are requested that in cases of emergency they contact the School Office first. This ensures that staff are aware of any potential issue and may make the necessary arrangements.
- Mobile devices should not be used in any manner or in any location that could cause disruption to the normal routine of the school.
- Pupils should protect their device numbers and social media accounts by giving details only to family. This will help protect the pupil's details from falling into the wrong hands and guard against insulting, threatening or unpleasant communications.
- The School recognises the importance of emerging technologies present in modern mobile. Teachers may wish to utilise these functions to aid teaching and learning and pupils may have the opportunity to use their mobile or smart devices in the classroom. On these occasions, express permission will be given by the teacher. Pupils may then use their mobile devices in the classroom for that lesson only. The use of personal mobile devices in one lesson for a specific purpose does not mean further usage is then acceptable.
- If asked to do so, pupils must show the content requested or hand their device to a member of staff or other designated adult including the police.
- The purpose of the use of personal devices in the classroom is strictly educational. Mobile devices can only be used for personal reasons if the pupil has been given permission by a teacher or another member of staff.
- All users agree not to exploit technology resources, interfere with another pupil's use of the resources, or use technology resources with the intent of causing harm to others.
- All pupils are required to ensure their personal devices are free from unsuitable material and any malicious content such as viruses and malware that may compromise the security of the school's network.
- To conform to Health and Safety compliance, any defective or damaged devices should not be brought into the school.

Theft or damage

- The responsibility for keeping a pupil's mobile device safe lies with the pupil; the School accepts no responsibility for replacing lost, stolen or damaged mobile devices.

- The School accepts no responsibility for pupils who lose or have their mobile devices stolen while travelling to and from school.
- Pupils should mark their mobile device clearly with their name or an identifiable detail.
- When a mobile device is found on school premises and the owner cannot be located, it should be handed into the School Office.
- It is strongly advised that pupils use passwords and/or pin numbers to ensure that unauthorised communications cannot be made on their devices (e.g. by other pupils, or if stolen). Pupils must keep their password/pin numbers confidential. Mobile devices and/or passwords must not be shared.
- Lost and stolen mobile devices in the U.K. can be blocked across all networks making them virtually worthless to the thief. Call your network provider as soon as possible after your device has been lost or stolen. This can be a temporary measure in case it is recovered.

Inappropriate conduct and content

- Using mobile devices to bully or threaten pupils or staff is unacceptable. Cyber-bullying will not be tolerated. In some cases it could constitute criminal behaviour. Using technology to humiliate, embarrass or cause offence will not be tolerated; regardless of whether 'consent' was given.
- It is forbidden for pupils to use their own or other pupils' mobile devices to take videos and pictures of acts to denigrate or humiliate others. This also includes using mobile devices to photograph or film any pupil or member of staff without their consent. It is a criminal offence to use a mobile device to menace, harass or offend another person; almost all communications can be traced.
- Mobile devices are not to be held or used in changing rooms or toilets or used in any situation that may cause embarrassment or discomfort to other pupils, staff or visitors to the school.
- Should there be any disruption to lessons caused by a mobile device, the responsible pupil may face disciplinary actions as sanctioned by the Deputy Head (Pastoral). This may include a mobile device ban in school for one, some or all pupils.
- It is unacceptable to take a picture of a member of staff without their permission. In the event that this happens the pupil will be asked and instructed to delete those images.
- Any pupil who uses vulgar, derogatory, or obscene language while using a mobile device will face disciplinary action as sanctioned by the Deputy Head (Pastoral).
- Pupils must ensure that files stored on their devices do not contain violent, degrading, racist or pornographic images. The transmission of such images is a criminal offence.
- It is the parents'/carer's responsibility to have spoken to their son or checked their device does not contain any harmful content before bringing it onto the school site.

Sanctions

- Pupils who infringe the rules set out in this document could face having their devices confiscated by staff. If the device is being used inappropriately the pupil must give it to a staff member if requested.
- On any infringement of this policy the mobile or smart device will be confiscated by the staff member and given to their form tutor.
- If a device is used by a pupil or member of staff such that the action raises a safeguarding concern, it will be reported to the DSL who may make a further referral Children's Services.
- If a device is used by a pupil or member of staff to commit a criminal act, including a breach of the Malicious Communications Act, then the police will be informed.

User agreement

By signing the School's Acceptable Use of BOYD Policy – Pupil Declaration/Parent declaration form, you agree to the following.

Pupils:

- You agree not to connect to any other wireless or network service that is outside of the school network (e.g., personal hotspot, VPN) when using your personal device on school premises.
- You agree to not download, share or store harmful content on your device.
- By using your own personal device in the school or during school visits and school activities, you agree that you understand this policy and that you agree to be bound to the rules, regulations and statements contained in this Policy.
- You also understand that the use of a personal device in school or for school activities is for learning purposes only and that it is a privilege, not a right to use your own personal device at school.
- You understand that you are fully responsible for the safety, security and care of your personal device when using it in school, during school visits and participation in outside activities.

Parents:

- You understand that More House School accepts no liability for any loss and/or damage to your children's personal devices that are used in school, during school visits and activities, or when in transit to and from the school.
- You understand that the decision to bring a personal device into the school rests with the parent/carer, as does the liability for any loss and/or damage that may occur as a result of using the personal device in school, during school visits and other outside activities.
- You understand that by allowing the pupil to bring their personal device into school, both you and the pupil agree to these terms and conditions and agree to be bound to the rules, regulations and statements contained in this Policy.

BOYD Acceptable Use agreement form

Pupil Name: **Signed (Pupil):**	**Date:**
Parent/carer agreement: Both pupils and their parents/carers are asked to sign declarations to show that they agree to follow this Acceptable Use Policy and have understood and agree with the content of the Mobile Device Policy. As the parent or legal guardian of the above pupil, I have read and understood the School's Mobile Device policy. • I am aware that my child has signed the BOYD Acceptable Use Policy We have discussed this document and my child agrees to follow the rules. • I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through 3G, 4G, 5G, VPNs or other mechanism outside of the school network. I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. • I have spoken to my child and I am confident his mobile device does not contain any harmful content. • I understand that if harmful content is found on my child's device the school has the right to confiscate their device and will contact any necessary external agencies as detailed in the school's safeguarding and child protection policy. • I understand the school is not liable for any damages for my child's device. • I will support the school by promoting safe use of the internet and digital technology at home and will inform the school if I have any concerns over my child's online-safety.	
Name: **Signed (parent/carer):**	**Date:**

Acceptable Use of IT Policy – Staff, and Supply Staff Declaration

This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of IT. All staff are expected to sign this policy and adhere to its contents at all times. Any concerns or clarification should be discussed with the Headmaster.

All staff must sign a copy of this Acceptable Use Policy for the Internet and return it to HR before access will be allowed.

- I appreciate that IT includes a wide range of systems, including mobile devices, tablets, digital cameras, email, social networking and that IT use may also include personal IT devices when used for school business.
- I understand that it is a criminal offence to use a school IT system for a purpose not permitted by its owner.
- I will only use the School's IT facilities and systems for professional purposes, or for uses deemed 'reasonable' by the Headmaster or Board of Governors.
- I will comply with the IT system security and not disclose any passwords provided to me by the School or other related authorities.
- I understand that I am responsible for all activity carried out under my username.
- I will only use the approved, secure email system for any school business.
- I will ensure that all electronic communications with parents, pupils and staff, including email, messaging and social networking, are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will ensure that personal data (such as data held on Engage) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Headmaster or Board of Governors.
- I will only take images of pupils and/or staff for professional purposes in line with school policy.
- I will not install any unauthorised software, or connect unauthorised hardware or devices to the school's network.
- I will not access, or attempt to access inappropriate material or illegal, including but not limited to material of a violent, criminal, offensive, discriminatory or pornographic nature (or create, share, link to or send such material).
- I will not access social networking sites (unless it is part of my role in the school) or chat rooms using school equipment.
- I will not use any improper language when communicating online, including in emails or other messaging services.
- I will respect copyright and intellectual property rights.
- I understand that all my use of the school's IT facilities and systems are monitored and logged and can be made available, on request, to the Headmaster and DSL.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support the school's Safe Use of Technology policy and help pupils to be safe and responsible in their use of IT and related technologies.
- I will promote online safety with pupils in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I will report any incidents of concern regarding children's safety to the DSL.
- I understand that sanctions for disregarding any of the above will be in line with the school's disciplinary procedures and serious infringements may be referred to the police.
- I will not share my password with others or log in to the school's network using someone else's details
- I will not share confidential information about the school, its pupils or staff, or other members of the community.
- I will not access, modify or share data I'm not authorised to access, modify or share
- I will not use the IT facilities for personal shopping, financial gain, gambling, political purposes or advertising.
- I will not take part in any activity that threatens the integrity of the school IT systems, or activity that attacks or corrupts other systems.

- I will let the DSL know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

The school will endeavour to ensure that staff will only be able to access approved sites.

The school reserves the right to examine or delete any files that may be held on its computer system, and to monitor all email & websites visited.

A deliberate breach of this policy will be dealt with as a disciplinary matter using the school's usual procedures.

Please confirm that you understand and accept this policy by signing below and returning the signed copy to the HR Department for authorisation and allocation onto the system.
Staff Name:
Staff Signature:
Date:

Acceptable Use of IT Policy – Guest, Governor and Contractor Declaration

- I understand that I have been given limited use of the school's IT facilities and systems as a temporary guest user.
- I understand that it is a criminal offence to use a school IT facilities and systems for a purpose not permitted by its owner, More House School.
- I will only use the school's IT facilities and systems for the purpose for which I have been given access.
- I will comply with the IT system's security and not disclose any passwords provided to me by the school or other related authorities.
- I will not install any hardware or software, unless approved for the execution of my duties.
- I will not access, or attempt to access inappropriate material or illegal, including but not limited to material of a violent, criminal, offensive, discriminatory or pornographic nature (or create, share, link to or send such material).
- I will not access social networking sites or chat rooms using school equipment.
- I will not use any improper language when communicating online, including in emails or other messaging services.
- I understand that all my use of the internet and other related technologies will be monitored and logged and can be made available, on request, to the Headmaster or my employer.
- I will respect copyright and intellectual property rights.
- I will let the DSL know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.
- I understand that if I disregard any of the above then it will be reported to my employer and serious infringements may be referred to external agencies as appropriate.

Please confirm that you understand and accept this policy by signing below and returning the signed copy to the HR Department for authorisation and allocation onto the system.
Staff Name:
Staff Signature:
Date:

Acceptable Use of IT Policy – Pupil Declaration (Junior)

When I use the school's IT systems in school I will:

- Always be responsible when I use the school's IT systems and internet.
- Ask a teacher or adult if I can do so before using them.
- Only use websites that a teacher or adult has told me or allowed me to use and not go on any inappropriate websites.
- Tell my teacher immediately if:
  - I click on a website by mistake
  - I receive messages from people I don't know
  - I find anything that may upset or harm me or my friends
  - I see anything that is unkind
- Only use school computers for school work and not personal use unless a teacher has said I can.
- Look after the school IT equipment and tell a member of staff straight away if something is broken or not working properly.
- Only use the username and password I have been given and not share them with anyone.
- Try my hardest to remember my username and password.
- Save my work on One Drive or Teams.
- Check with my teacher before I print anything.
- I will make sure that all messages I send are responsible and sensible. I know that emails might be shared with people I did not send them to.
- I will be polite and understand that other people might not think the same as me. I must respect their ideas and not be rude or disrespectful.
- Respect other's work and property and will not access, copy, remove or change another person's files without their permission.
- Log off or shut down a computer when I have finished using it.

I will not:

- Use the school computers to break rules.
- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites.
- Be unkind to others and not upset or be rude to them or bully them.
- Send messages without my own name or with a wrong name.
- Download or install software on the school network.
- Share my password with anyone, including my friends.
- Give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer.
- Send any photos, videos or live streams of people (including me) who aren't wearing all of their clothes even if they have given permission.
- Log in to the school's network using someone else's details.
- Use IT systems at school to make money for me.
- Arrange to meet anyone offline that I have met online without first asking my parent/carer, or without adult supervision.

I understand that the school will monitor my use of the school's IT systems and devices. This is so that they can help keep me safe and make sure I'm following the rules.

I understand that the school can give me consequences if I do unacceptable things online, even if I'm not in school when I do them.

MORE HOUSE SCHOOL

POLICY

SAFE USE OF TECHNOLOGY

Pupil Name: **Signed (Pupil):**	**Date:**

Parent/carer agreement:
All pupils use computer facilities, including internet access, as an essential part of their learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign declarations to show that they agree to follow this Acceptable Use Policy and have understood and agree with the content of the Safe Use of Technology Policy.

As the parent or legal guardian of the above pupil, I have read and understood the published school Safe use of Technology Policy and grant permission for my child to have access to use the internet, school email system, learning platform and other IT facilities at school.

- I am aware that my child has signed the Acceptable Use of IT Policy. We have discussed this document and my child agrees to follow the online-safety rules and to support the safe and responsible use of IT at More House School.
- I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access email, employing appropriate teaching practice and teaching online-safety skills to pupils.
- I understand that the school can check my child's computer files and the internet sites that they visit, and that if they have concerns about their online-safety or e-behaviour they will contact me.
- I understand the school is not liable for any damages arising from my child's use of the internet facilities.
- I will support the school by promoting safe use of the internet and digital technology at home and will inform the school if I have any concerns over my child's online-safety.

Name: **Signed (parent/carer):**	**Date:**

Acceptable Use of IT Policy – Pupil Declaration (Senior)

When I use the school's IT systems in school I will:

- I will always be responsible when I use the school's IT systems and internet.
- Ask a teacher or adult if I can do so before using them.
- Only use websites that a teacher or adult has told me or allowed me to use and not go on any inappropriate websites.
- Tell my teacher immediately if:
    - I click on a website by mistake
    - I receive messages from people I don't know
    - I find anything that may upset or harm me or my friends
    - I see anything that is unkind
- Only use school computers for school work and not personal use unless I have had permission from a teacher.
- Look after the school IT equipment and tell a member of staff straight away if something is broken or not working properly.
- Only use the username and password I have been given and not share them with anyone.
- Try my hardest to remember my username and password.
- Save my work on One Drive or Teams.
- Check with my teacher before I print anything.
- I will make sure that all messages I send to teachers or others are responsible and sensible. I know that emails might be shared with people I did not send them to.
- I will be polite and understand that other people might not think the same as me. I must respect their ideas and not be rude or disrespectful.
- Respect other's work and property and will not access, copy, remove or alter another person's files without their permission.
- I ensure that I have permission to use the original work of others in my own work
- Take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- Log off or shut down a computer when I have finished using it.

I will not:

- Use the school computers to break rules.
- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites.
- Be unkind to others and not upset or be rude to them or bully them.
- Send messages without my own name or with a wrong name.
- Download or install software on the school network.
- Try to get around the school firewall and security settings.
- Share my password with anyone, including my friends.
- Give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer.
- Send any photos, videos or live streams of people (including me) who aren't wearing all of their clothes even if they have given permission.
- Log in to the school's network using someone else's details.
- Use IT systems at school to make money for me.
- Try to download copies (including music and videos) where work is protected by copyright.
- Arrange to meet anyone offline that I have met online without first consulting my parent/carer, or without adult supervision.

MORE HOUSE SCHOOL

POLICY

SAFE USE OF TECHNOLOGY

I understand that the school will monitor my use of the school's IT systems and devices. This is so that they can help keep me safe and make sure I'm following the rules.

I understand that the school can give me consequences if I do unacceptable things online, even if I'm not in school when I do them.

Pupil Name: **Signed (Pupil):**	**Date:**

Parent/carer agreement:
All pupils use computer facilities, including internet access, as an essential part of their learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign declarations to show that they agree to follow this Acceptable Use Policy and have understood and agree with the content of the Safe Use of Technology Policy.

As the parent or legal guardian of the above pupil, I have read and understood the published school Safe use of Technology Policy and grant permission for my child to have access to use the internet, school email system, learning platform and other IT facilities at school.

- I am aware that my child has signed the Acceptable Use of IT Policy. We have discussed this document and my child agrees to follow the online-safety rules and to support the safe and responsible use of IT at More House School.
- I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access email, employing appropriate teaching practice and teaching online-safety skills to pupils.
- I understand that the school can check my child's computer files and the internet sites that they visit, and that if they have concerns about their online-safety or e-behaviour they will contact me.
- I understand the school is not liable for any damages arising from my child's use of the internet facilities.
- I will support the school by promoting safe use of the internet and digital technology at home and will inform the school if I have any concerns over my child's online-safety.

Name: **Signed (parent/carer):**	**Date:**