# E-Safety Policy

## (Including Acceptable Use Policy for Pupils)

## 2023-2024

**Author:**
C Phelps, Deputy Head Pastoral
**Approved by the Governing Board:**
September 2023
**Date of next review:**
July 2024

MORE HOUSE SCHOOL
KNIGHTSBRIDGE

## Contents Page

# Policy Statement

At More House School, and in keeping with the Keeping Children Safe in Education ("KCSIE") 2023 guidance, we believe it is essential that pupils are safeguarded from potentially harmful and inappropriate online material. We have a 'whole School approach' to online safety which empowers us to protect and educate pupils and staff in their use of technology.

More House School acknowledges that the internet and associated Bring Your Own Device (''BYOD'') initiative, such as, computers, laptops, tablets et al, will provide a creative and engaging platform from which pupils can learn and flourish and is an important aspect of everyday life.

More House School believes that pupils should be empowered to build resilience and to develop strategies to manage and respond to risk online.

This policy applies to all staff including the Governing Board, Senior Leadership Team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the School (collectively referred to as "staff" in this policy) as well as pupils and parents.

This policy applies to all access to the internet and use of any form of technology within School, including personal devices/BYOD, or where pupils, staff or other individuals have been provided with School issued devices for use off-site, such as work laptops, tablets or mobile phones.

A 'whole School approach' to online safety is essential to safeguarding. Our E-safety measures include robust policies and procedures, effective training, education for staff, pupils and parents, robust technical solutions to allow pupils to access appropriate resources and ongoing review and evaluation of the systems in place. To safeguard students from potentially harmful and inappropriate material online, the School has appropriate filtering and monitoring systems in place, which carefully monitor without an unreasonable level of blocking.

We consult with stakeholders (pupils, staff and parents) on the formation of policies and procedures. Online safety is evident in the curriculum through our RSE and PHSE programme, the EMC$^2$ curriculum and assembly programme.
Furthermore, the Catholic ethos of the School enshrines our values of dignity, respect, equality, justice, love and tolerance which guides the behaviour of all, both on and offline.

## 1. Aims:

Our School aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors;
- Identify and support groups of pupils that are potentially at greater risk of harm online than others;
- 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 (which we refer to as 'mobile phones');
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate;

- Ensure that the curriculum teaches the knowledge and behaviours necessary for our pupils to flourish online and rewards pupils who model the knowledge and behaviours appropriately, and
- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.

The 4 key categories of risk:

The issues classified within e-Safety are considerable and vast, but can be broadly categorised into **four areas of risk:**

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism;

- **Contact** – being subjected to harmful online interaction with other users, such as child-to-child 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 scams.

This policy aims to ensure that all members of the School community are aware of these risks and can take the appropriate measures to safeguard themselves and others online.

# 2. Legislation and guidance

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

- Teaching online safety in Schools;
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff;
- Relationships and sex education;
- Searching, screening and confiscation;
- UK Safer Internet Centre - appropriate filtering and monitoring, and
- E-security guidance: Available from the National Education Network (NEN).

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

# 3. Communicating School Policy

This policy is available from the School office and on the School website for parents, staff, and pupils to access when and as they wish. Rules relating to the School code of conduct when online, and e-safety guidelines, are displayed around the School and are reflected in our Safeguarding and Child Protection Policy. E-safety is integrated into the curriculum in our whole School approach and during EMC$^2$ lessons and form time where personal safety, responsibility, and/or development are being discussed through PSHE and RSE.

# 4. Roles and Responsibility

## 4.1 The Governing Board

The Governing Board has overall responsibility for monitoring this policy and holding the Head to account for its implementation.

The Governing Board will 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 Governing Board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The Governing Board will coordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The Governing Board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

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 will receive feedback from the lead of the Cyber group (Ms Faith Hagerty) of what needs to be done to support the School in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- 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 they have read and understand this policy;
- Agree and adhere to the terms on acceptable use of the School's ICT systems and the internet (appendix 2);
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures, and
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of 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

## 4.2 The Head's responsibility

- Oversee the update and review of the E-safety policy and manage allegations of misuse of ICT by staff;
- Ensure that the School e-Safety practice (and as a significant safeguarding issue), is in keeping with legal requirements;
- Ensure there are appropriate and up-to-date policies working in conjunction with the E safety policy such as the Safeguarding and Child Protection Policy and Behaviour and Discipline Policy;
- Ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of the School's systems and networks;
- Ensure that e-Safety is embedded within the curriculum, which enables all pupils to develop an age-appropriate understanding of e-Safety;
- Support the DSL and deputies by ensuring they have sufficient time and resources to fulfil their e-Safety responsibilities;
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, and
- Audit and evaluate E-Safety practice to identify strengths and areas for improvement.

## 4.3 The DSL's responsibility

Details of the School's designated safeguarding lead (DSL) and deputies (DDSLs) are set out in our Safeguarding and Child Protection Policy, as well as relevant job descriptions.

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

- Supporting the Head in ensuring that staff understand this policy and that it is being implemented consistently throughout the School;
- Working with the Head and Governing Board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly;
- Taking the lead on understanding the filtering and monitoring systems and processes in place on School devices and School networks;
- Working with the ICT manager to make sure the appropriate systems and processes are in place;
- Working with the Head, ICT manager and other staff, as necessary, to address any online safety issues or incidents;
- 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 and dealt with appropriately in line with this policy;
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the School's Behaviour and Discipline Policy;
- Working alongside the Deputy Head Academic/ICT Coordinator to provide updates and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs)

- Liaising with other agencies and/or external services if necessary;
- Supporting the Cyber group to provide regular reports on online safety in School to the Head and/or Governing Board;
- Working alongside the Deputy Head Academic/ICT Coordinator to undertake annual risk assessments that consider and reflect the risks children face;
- Working alongside the Deputy Head Academic/ICT Coordinator to ensure that e-Safety is embedded as part of the School's safeguarding responsibilities and that a whole School approach is implemented;
- Accessing regular and appropriate training and support to ensure staff understand the unique risks associated with e-Safety required to keep pupils safe online whilst recognising the particular vulnerabilities of those pupils with Special Educational Needs (SEND);
- Maintain records of e-Safety concerns, as well as actions taken, as part of the School's safeguarding recording mechanisms;
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy;
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the School's Behaviour and Discipline Policy, and
- 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.

This list is not intended to be exhaustive.

## 4.4 The ICT Technician

The ICT Technician is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on School devices and School networks, which are reviewed and updated at least annually 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;
- Ensuring that the School's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly;
- Conducting an annual security review and monitor the school's ICT systems on a monthly basis;
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files;
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy;
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

This list is not intended to be exhaustive.

## 4.5 All staff and volunteers

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

- Reading and adhering to the E-Safety policy and acceptable use policies;
- Taking responsibility for the security of the School systems and the data they use or have access to;
- Modelling good practice when using technology and maintaining a professional level of conduct in their personal use of technology, both on and offsite.
- Agreeing and adhering to the terms on acceptable use of the School's ICT systems and the internet (Appendix 2), and ensuring that pupils follow the School's terms on acceptable use (Appendix 1);
- Embedding E-Safety education in curriculum delivery. By way of example, now that the BYOD initiative is in place, classroom teachers must ensure pupils are using their devices appropriately and only for the activities authorised by the classroom teacher;
- Addressing any inappropriate BYOD issues that arise in their classroom by first sanctioning the pupil and/or escalating the inappropriate usage to the Head of Department ("HOD"). If the HOD feels that this is a serious infraction or an E-safety concern, it will be escalated to the DSL and/or deputies;
- Having an awareness of a range of E-Safety issues and how they may be experienced by the pupils in their care;
- Identifying E-Safety concerns (including cyber-bullying) and taking appropriate action by following the School's safeguarding and behaviour and discipline policies and procedures;
- Responding appropriately to all reports and concerns about sexual violence and/or harrassment, both online and offline and maintaining an attitude of 'it does happen here'. Further guidance can be found in Section 10.3 of this policy;
- Knowing when and how to escalate E-Safety issues, including signposting to appropriate support, internally and externally, and
- Taking personal responsibility for professional development in this area.

This list is not intended to be exhaustive.

## 4.6 Deputy Head Academic

The Deputy Head Academic is responsible for:

- Ensuring e-safety is evident across the curriculum, and
- Providing training for students and staff (whether in-house or via external agencies).

## 4.7 Parents

It is the responsibility of parents to:

- Read the acceptable use policies and to ensure that their daughters adhere to them;
- Support the School's E-Safety approaches by discussing E-Safety issues with their daughter and reinforcing appropriate and safe online behaviours at home;

- Manage and oversee their daughter's online usage, behaviour, language and the apps that she uses and posts on;
- Consider operating a time restriction, beyond which their daughter has no access to technology and can relax and unwind before bedtime e.g. for KS3 no technology after 8pm; KS4 no technology after 9pm;
- Role model safe and appropriate use of technology and social media;
  Identify changes in behaviour that could indicate that their daughter is at risk of harm online;
- Seek help and support from the School, or other appropriate agencies, if their daughter encounters risk or concerns online, and
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

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

## 4.8 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet 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 on acceptable use (appendix 3).

## 4.9 Pupils

It is the responsibility of pupils to:

- Follow the instructions of classroom teachers at all times and to use and access the online sites/materials and resources that teachers have authorised the pupils to access and use. Pupils agree to engage in age appropriate E-Safety education opportunities;
- Read and adhere to the acceptable use policies;
- Always be respectful, kind and considerate and to uphold each person's dignity both on and offline;
- Take responsibility for keeping themselves and others safe online;
- Contribute to the development of E-Safety policies by providing feedback through pupil questionnaires and School Council feedback, and
- (Year 7-11 students) Turn off any smart phone or watch that may provide them with unlimited and unrestricted access to the internet through networks (i.e. 3G, 4G and 5G) and hand this to the form tutor at the start of the School day.

The School accepts no responsibility for the loss, theft or damage of such items on our premises.
Years 7-11 pupils are **not allowed** to use their devices outside of lessons and are **not permitted** to use their devices at break and/or lunchtime. The only exception to this is if pupils are in the **library during break and/or lunchtime** to complete School work and under the supervision of a member of staff. Pupils must ensure their personal devices and/or School devices are either in lockers or in their School bags during break and lunch. Mobile phones will be handed in at the start of the School day and stored with the Pastoral Support Officer.

# 5. Education

## 5.1 Educating pupils about online safety

Pupils will be taught about online safety as part of the EMC$^2$ curriculum.

The following topics will be covered in the Spring Term across KS3:

- Self-image and identity
- Online relationships
- Online Reputation
- Online Bullying
- Managing online information
- Health, well-being and lifestyle
- Privacy and security
- Copyright and ownership

Pupils will be taught about online safety as part of the Relationship and Sex Education (RSE) and PSHE curriculum.

In Key Stage 3:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in Key Stage 4 will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

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, victims of abuse and pupils with SEND.

By the **end of secondary school**, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online;
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online;
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them;
- What to do and where to get support to report material or manage issues online;
- The impact of viewing harmful content;
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners;
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail;
- How information and data is generated, collected, shared and used online;
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours, and

- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online).

## 5.2 Educating parents about online safety

The School will raise parents' awareness of internet safety in letters or other communications home, and in information via our website or weekly newsletters. This policy will also be shared with parents.

The School will let parents know:

- What systems the School uses to filter and monitor online use, and
- (*When working remotely*) what their children are being asked to do online, including the sites they will be asked to access and who from the School (if anyone) their child will be interacting with online

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

Concerns or queries about this policy can be raised with any member of staff or the Head.

# 6. Cyber-bullying

## 6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the School Behaviour and Discipline Policy and Anti Bullying Strategy)

## 6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The School will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Tutors will discuss cyber-bullying with their tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training. (see section 11 for more detail).

The School also sends information/leaflets on cyber-bullying to parents either directly or through the weekly newsletter so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the School will follow the processes set out in the School's Behaviour and Discipline policy. Where illegal, inappropriate or harmful

material has been spread among pupils, the School will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if there are reasonable grounds to suspect that possessing that material is illegal. The DSL will also work with external services if it is deemed necessary to do so.

## 6.3 Examining electronic devices

The Head, and any member of staff authorised to do so by the Head, can 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 a Senior member of staff;
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it, and
- 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 or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break the school code of conduct

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

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

- The DfE's latest guidance on searching, screening and confiscation;
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people, and
- Search and Confiscation Policy.

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

### 6.4 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 others. For example, in the form of 'deep fakes', 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 pupils in line with our Behaviour and Discipline 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.

## 7. Acceptable use of the Internet in School

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (Appendix 1 and Appendix 2). 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 and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendix 1 and 2.

## 8. Making use of BYOD, ICT and the Internet in School

The BYOD to School initiative and use of the internet withinin the School aim to raise educational standards, promote pupil achievement, support the professional work of staff and enhance the School's management functions. Technology is advancing rapidly and is

now a huge part of everyday life, education and business. We want to equip our students with all the necessary ICT skills that they will need in order to enable them to progress confidently into a professional working environment when they leave School. Some of the benefits of using ICT and the internet in Schools are:

## 8.1 For students

- Access to worldwide educational resources and institutions such as art galleries, museums and libraries;
- Contact with Schools in other countries resulting in cultural exchanges between pupils all over the world;
- Access to subject experts, role models, inspirational people and organisations. The internet can provide a great opportunity for pupils to interact with people whom they otherwise would never be able to meet;
- An enhanced curriculum; interactive learning tools; collaboration - locally, nationally, and globally; self-evaluation; feedback and assessment; updates on current affairs as they happen;
- Access to learning whenever and wherever convenient;
- Freedom to be creative;
- Freedom to explore the world and its cultures from within a classroom;
- Social inclusion, in class and online;
- Access to case studies, videos and interactive media to enhance understanding, and
- Individualised access to learning.

## 8.2 For staff

- Professional development through access to national developments, educational materials and examples of effective curriculum practice and classroom strategies;
- Immediate professional and personal support through networks and associations;
- Improved access to technical support;
- Ability to provide immediate feedback to students and parents, and
- Class management, attendance records, schedule, and assignment tracking.

## 8.3 For parents

- Access to resources to support their daughter's learning;
- Access to the parent portal and information published on that platform such as reports and assessment results;
- Access to the School website;
- Effective communication with the School via email;
- Receiving texts from the School, and
- Reporting absence to the School.

## 8.4 Classroom Use

- The School's 'Bring Your Own Device' ("BYOD") initiative incorporates a wide range of technology. This includes School and personal access to:
    - Computers, laptops and other BYOD/digital devices;
    - Internet which may include search engines and educational websites;
    - Google Classroom;
    - Email and School Gmail accounts;
    - Games-based technologies; and
    - Digital cameras, webcams and video cameras.
- All School owned devices and BYOD will be used in accordance with the acceptable use policies and with appropriate safety and security measures in place;
- Members of staff will always evaluate websites, tools and applications fully before use in the classroom or recommending for use at home, Google Slides and Google Docs containing links will include the date that the links were last checked;
- We will use age-appropriate search tools to identify which tool best suits the needs of our community;
- Members of staff will ensure that the use of internet-derived materials, by staff and pupils complies with copyright law and acknowledge the source of information;

- Classroom teachers are responsible for the supervision of pupils' usage of the BYOD and will ensure that they are accessing information, websites, appropriate to their age and ability;
- During remote learning, teaching staff will communicate to parents what online sites their daughters will be asked to access, and who their daughter will be interacting with online;
- More House School's IT Support Manager has ensured that the School has age and ability appropriate filtering and monitoring in place, to limit pupil exposure to online risks;
- The IT Technician is aware of the need to prevent "over blocking", as that may unreasonably restrict what can be taught, with regards to online activities and safeguarding;
- As previously stated, all members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard pupils; effective BYOD classroom management and regular education about safe and responsible use is essential, and
- Year 7-11 pupils are only allowed to use their BYOD during lessons and in the **library during break and/or lunchtime** for the completion of School work. This will be supervised by a break and lunchtime member of staff. Pupils must ensure their personal devices and/or School devices are either in lockers or in their School bags during break and lunch.

# 9. Staff using work devices 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 with family or friends, and
- Keeping operating systems up to date by always installing the latest updates.

Staff members must not use the device in any way which would violate the School's terms of acceptable use, as set out in Appendix 2.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the ICT technician.

# 10. How the School will respond to issues of misuse

Where a pupil misuses the School's ICT systems or internet, we will follow the procedures set out in our Behaviour and Discipline policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

All members of the More House School staff will be made aware of the reporting procedure on CPOMS for online safety concerns, including but not limited to:

- breaches of filtering, youth produced sexual imagery (sexting), cyberbullying, child on child abuse, prejudice, discriminatory behaviour, and illegal content;

- consideration by the DSL as to whether the incident is a safeguarding or behavioural incident, and
- taking the relevant steps to support the students involved.

We require staff, parents and pupils to work in partnership to resolve online safety issues.

After any investigations are completed, the DSL will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
If we are unsure how to proceed with an incident or concern, the DSL will seek advice from the relevant external agencies.

Where there is suspicion that illegal activity has taken place, the DSL will contact the relevant external agencies and/or the Police if there is immediate danger or risk of harm.

If an incident or concern needs to be passed beyond our community (for example if other local schools are involved or the public may be at risk), the DSL will speak with the Police.

## 10.1 Concerns about Pupils' Welfare

- The DSL or DDSL will be informed of any online safety incidents involving Safeguarding or Child Protection concerns through immediate alerts sent through Smoothwall Alerts. The DSL or DDSL will keep the Head informed and the Head will be involved in addressing any serious concerns/matters pertaining to this;
- The DSL or DDSL will make a record of the concern on CPOMS; all concerns will contain the following:
    - a clear and comprehensive summary of the concern;
    - details of how the concern was followed up and resolved, and
    - a note of any action taken, decisions reached and the outcome.
- The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the KCSIE (2023) and the School Safeguarding and Child Protection Policy, and
- The DSL and/or Deputy DSLs will inform parents of online safety incidents or concerns involving their daughter, as and when required.

## 10.2 Cyber Bullying/Child on Child Abuse

More House School operates under the culture that '*this (online/cyberbullying and/or child on child abuse) could happen here'* and thus we treat any issues, concerns, allegations, reports pertaining to online/cyberbullying very seriously and in line with the procedures above. All our approaches are underpinned by the principle that there is a zero-tolerance approach to bullying and child on child abuse and that bullying is never acceptable and will not be tolerated. We act with '*the best interests of the child*' as the guiding principle.

Cyberbullying, prejudice based bullying, discriminatory bullying, child on child abuse, online bullying, sexual harassment and sexual bullying and online bullying, is taken very seriously by the School. This policy should be read in conjunction with the Anti-Bullying Strategy, the Sexual Violence and Sexual Harassment Policy and the Behaviour and Discipline Policy.

All members of the School community know what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action.

Instances of alleged misconduct / inappropriate online behaviour / bullying should be reported to the Deputy Head Pastoral immediately.

Staff will make a record on CPOMS of what has been reported to them. All cases of bullying (whether in School or online) will contain the following:

- a clear and comprehensive summary of the concern;
- details of how the concern was followed up and resolved, and
- a note of any action taken, decisions reached and the outcome.

If an allegation of bullying does occur, the School will:

- take it seriously;
- act as quickly as possible to establish the facts. It may be necessary to examine School systems and logs or contact the service provider in order to identify the bully;
- record and report the incident on CPOMS, as outlined above;
- provide support and reassurance to the victim, and
- make it clear to the 'bully' that this behaviour will not be tolerated. If there is a group of people involved, they will be spoken to individually and as a whole group. It is important that children who have harmed another, either physically or emotionally, redress their actions and the School will make sure that they understand what they have done and the impact of their actions.

If a sanction is used, it will correlate to the seriousness of the incident and the 'bully' will be told why it is being used. They will be asked to remove any harmful or inappropriate content that has been published, and the service provider may be contacted to do this if they refuse or are unable to remove it. They may have their internet access suspended in School.

Repeated bullying may result in a fixed-term exclusion, issued by the Head.

## 10.3 Online Sexual Violence and Sexual Harassment Between Children

More House School operates under the assumption that '*this could happen here*' and thus we treat any issues, concerns, allegations and reports very seriously and in line with the procedures noted above. All our approaches are underpinned by the principle that there is a zero-tolerance approach to sexual violence and sexual harassment and it is never acceptable and will not be tolerated.

The School recognises that sexual violence and sexual harassment between children can take place online. Examples may include but are not limited to: consensual and non-consensual sharing of nudes and semi-nudes, sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation. Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our policies on Sexual Violence and Sexual Harrassment, Behaviour and Discipline, Safeguarding and Child Protection and our Anti-bullying Strategy.

As per Part One of Keeping Children Safe in Education, if More House staff have any concerns about a pupil's welfare, they will act on them immediately and report it to the DSL.

## 10.4 Online Sexual Abuse and Child Sexual Exploitation (CSE) and Child Criminal Exploitation (CCE)

Both CSE and CCE are forms of abuse that occur where an individual or group takes advantage of an imbalance in power to coerce, manipulate or deceive a child into taking part in sexual or criminal activity, in exchange for something the victim needs or wants, and/or for the financial advantage or increased status of the perpetrator or facilitator and/or through violence or the threat of violence. CSE and CCE can affect pupils, and can

include children who have been moved (commonly referred to as trafficking) for the purpose of exploitation.

The School will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.

The School recognises online child sexual abuse and exploitation (including child criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL in conjunction with the Head. Please refer to the Sexual Violence and Sexual Harassment Policy for further guidance.

External agencies and/or the police will be contacted where necessary.

## 10.5 Indecent Images of Children (IIOC)

The School will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC). We will always act in accordance with the School's Safeguarding and Child Protection Policy.

We will respond to concerns regarding IIOC on School equipment and/or BYOD equipment, even if access took place off site.

If we are unclear if a criminal offence has been committed, the DSL, in conjunction with the Head, will obtain advice immediately from the Police.

## 10.6 Online Hate

Online hate content, directed towards, or posted by, specific members of the community will not be tolerated and will be responded to in line with existing policies, including Anti-bullying and Behaviour and Discipline.

If we are unclear on how to respond, or as to whether a criminal offence has been committed, the DSL will obtain advice through the relevant external agencies and/or the Safer Schools Officer.

## 10.7 Online Radicalisation and Extremism

The School will take all reasonable precautions to ensure that pupils and staff are safe from terrorist and extremist material when accessing the internet on site.

If we are concerned that a pupil may be at risk of radicalisation online, the DSL will be informed immediately and action will be taken in line with our Safeguarding and Child Protection Policy.

If we are concerned that a member of staff may be at risk of radicalisation online, the Head will be informed immediately.

Relevant external agencies will be contacted where necessary.

## 10.8 Staff Misuse

Where a staff member misuses the School's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the Staff Code of Conduct.

- Any complaint and/or allegation about staff misuse will be referred to and investigated by the Head.
- Appropriate action/sanctions will be taken by the Head in accordance with our Safeguarding and Child Protection Policy for Managing Allegations against Staff and Behaviour and Discipline policies.

The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The School will consider and take advice from relevant external agencies, whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

# 11. Emails

Access to the School's email systems will always take place in accordance with data protection legislation and in line with other policies including (but not limited to) the: Policy on Behaviour and Discipline, Safeguarding and Child Protection Policy and the Employee Handbook.

The School uses email internally for staff and pupils, and externally for contacting pupils and parents, and it is an essential part of School communication. It is also used to enhance the curriculum by:

- initiating contact and projects with other Schools nationally and internationally, and
- providing immediate feedback on work, and requests for support where it is needed.

Staff and pupils should be aware that School email accounts should only be used for School-related matters, i.e for staff to contact parents, pupils, other members of staff and other professionals for work purposes. This is important for confidentiality. The School has the right to monitor emails and their contents but will only do so if it feels there is reason to.

## 11.1 School email accounts and appropriate use

All pupils and staff are assigned an individual gmail account when they join the School. Only these accounts, which are managed and approved by the School, may be used.

Staff should be aware of the following when using email in School:

- Staff should only use official School-provided email accounts to communicate with pupils, parents or carers. Personal email accounts should not be used to contact any of these people and should not be accessed during School hours;
- Emails sent from School accounts should be professionally and carefully written. Staff are representing the School at all times and should take this into account when entering into any email communications;
- Staff must tell their manager or a member of the Senior Leadership Team if they receive any offensive, threatening or unsuitable emails either from within the School or from an external account. They should not attempt to deal with this themselves;
- The forwarding of chain messages is not permitted in School, and
- Staff should only use pupil initials in email subject titles.

Pupils should be aware of the following when using email in School, and will be taught to follow these guidelines through the ICT curriculum and in any instance where email is being used within the curriculum or in class:

- In School, pupils should only use their School email address;
- Pupils will make use of acceptable email etiquette when emailing their teachers. This includes an appropriate salutation, use of correct grammar, appropriate register and a suitable sign off;
- Excessive social emailing will be restricted;
- Pupils should tell a member of staff if they receive any offensive, threatening or unsuitable emails either from within the School or from an external account. They should not attempt to deal with this themselves, and
- Pupils must be careful not to reveal any personal information over email, or arrange to meet up with anyone who they have met online without specific permission from an adult in charge. Pupils will be educated through the ICT curriculum to identify spam, phishing and virus emails and attachments that could cause harm to the School network or their personal account or wellbeing.

### 11.2 Passwords and Password Security

Passwords for School gmail accounts are strictly controlled and managed by the IT department. Should a password be inadvertently shared or forgotten, the pupil or staff member should contact the IT department who will reset the password.

## 12. Published content and the School website

The School website is viewed as a useful tool for communicating our School ethos and practice to the wider community. It is also a valuable resource for parents, students, and staff for keeping up-to-date with School news and events, celebrating whole-School achievements and personal achievements, and promoting School projects. The website is in the public domain, and can be viewed by anybody online. We will ensure that all images and videos shared online are used in accordance with the associated policies, including (but not limited to) the: Policy on Behaviour and Discipline, Safeguarding and Child Protection Policy and Data Protection Policy. Any information published on the website will be carefully considered in terms of safety for the School community, copyrights and privacy policies. No personal information on staff or pupils will be published, and details for contacting the School will be for the School office only. For information on the School policy on children's photographs on the School website please refer to Section 12.1 and 12.2 of this policy.

The Marketing and Office Manager is responsible for publishing and maintaining the content on the School website.

### 12.1 Policy and guidance of safe use of children's photographs and work

Colour photographs and pupils' work bring our School to life, showcase our student's talentsand add interest to publications both online and in print that represent the School. However, the School acknowledges the importance of having safety precautions in place to prevent the misuse of such material. The School will only use photographs in accordance with its Privacy Notice. On a pupil's admission to the School, parents/carers will be asked to sign a photography consent form. The School does this so as to prevent repeatedly asking parents for consent over the school year, which is time-consuming for both parents and the School. The terms of use of photographs never change, and so consenting to the

use of photographs of their daughter over a period of time rather than a one-off incident does not affect what parents are consenting to.

Parents will be contacted annually for consent.

## 12.2 Using photographs of individual children

The vast majority of people who take or view photographs or videos of children do so for entirely innocent, understandable and acceptable reasons. Sadly, some people abuse children through taking or using images, so we must ensure that we have some safeguards in place. It is important that published images do not identify students or put them at risk of being identified. The School is careful to ensure that images published on the School website cannot be reused or manipulated through watermarking and browser restrictions.

Only images created by or for the School will be used in public and children may not be approached or photographed while in School or doing school activities without the School's permission. The School follows general rules on the use of photographs of individual children:

- Parental consent must be obtained. Consent will cover the use of images in:
    - all School publications;
    - on the School website or in newspapers as allowed by the School; and
    - in videos made by the School or in class for School projects.
- We will store photographs and videos of children securely, in accordance with our safeguarding policy and data protection law. We will keep hard copies of images in a locked drawer and electronic images in a protected folder with restricted access;
- Images will be stored for a period of 10 years. We will never store images of children on unencrypted portable equipment such as laptops, memory sticks and mobile phones. More House does not permit staff and volunteers to use any personal equipment to take photos and recordings of children. Only cameras or devices belonging to the School should be used.
- Names of stored photographic files will not identify the pupil.
- Images will be carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that pupils are appropriately dressed. Photographs of activities which may pose a greater risk of potential misuse (for example, swimming activities), will focus more on the sport than the pupils (ie a student in a swimming pool, rather than standing by the side in a swimsuit).
- For public documents, including in newspapers, full names will not be published alongside images of the pupil. Groups may be referred to collectively by year group or form name;
- Events recorded by family members of the students such as School plays or sports days must be used for personal use only;
- Parents will be asked for photos taken during School events not to be shared on social media, recommending that people check the privacy settings of their social media account to understand who else will be able to view any images they share;
- Pupils are encouraged to tell a member of staff if they are concerned or uncomfortable with any photographs that are taken of them or they are being asked to participate in, and
- Any photographers who are commissioned by the School will be fully briefed on appropriateness in terms of content and behaviour, will wear identification at all times, and will not have unsupervised access to the pupils. For more information on safeguarding in School please refer to our School Safeguarding and Child protection Policy.

## 12.3 Complaints of misuse of photographs or video

Parents should follow the School's Complaints Policy if they have a concern or complaint regarding the misuse of School photographs. Please refer to our Complaints Policy for more information on the steps to take when making a complaint. Any issues or sanctions will be dealt with in line with the School's Safeguarding and Child Protection Policy and Policy on Behaviour and Discipline.

## 12.4 Social networking, social media and personal publishing

The expectations regarding safe and responsible use of social media apply to all members of the More House School community. The term social media may include, but is not limited to, blogs, Tiktok, Snapchat, Wikis, social networking sites, bulletin boards, chat rooms and instant messaging programmes. These online forums are the more obvious sources of inappropriate and harmful behaviour and where pupils are most vulnerable to being contacted by a dangerous person. SEND pupils are particularly vulnerable to cyber bullying and online grooming and Form Tutors and the Deputy Head Pastoral in consultation with the SENCO will ensure that these pupils fully understand the risks they face online through one to one sessions and information given in form time. It is important that we educate students so that they can make their own informed decisions and take responsibility for their conduct online. There are various restrictions on the use of these sites in School that apply to both students and staff.

Social media sites have many benefits for both personal use and professional learning; however, both staff and students should be aware of how they present themselves online. Students are taught through the ICT curriculum and PSHE and RSE programmes about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place.

The School follows general rules on the use of social media and social networking sites in School:

- Pupils are educated on the dangers of social networking sites and how to use them in safe and productive ways. They are all made fully aware of the School's Code of Conduct regarding the use of ICT and technologies and behaviour online;
- Any sites/resources that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use;
- Official School blogs created by staff or students/year groups/School clubs as part of the School curriculum will be password-protected and run from the School website with the approval of a member of staff and will be moderated by a member of staff;
- Pupils and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The School expects all staff and pupils to remember that they are representing the School at all times and must act appropriately, and
- Safe and professional behaviour of staff online will be discussed at staff induction and training sessions.

## 12.5 Pupil Work

All work is securely stored in Google Classroom.

# 13. Mobile phones and Smart devices including smart watches

**Because Year 7-11 pupils will now use their own device in many lessons pupils are NOT permitted to have their mobile phones and/or smart devices such as apple watches in lessons** *(unless the classroom teacher has given permission and in this instance, the classroom teacher is responsible for taking the phone box from the office and crucially in returning it to the office at the end of the lesson to ensure all pupils have returned their mobile phone and/or smart watch***).** This is for a number of reasons:

- they can make pupils and staff more vulnerable to cyberbullying;
- they can be used to access inappropriate internet material;
- they can be a distraction in the classroom;
- they are valuable items that could be stolen, damaged, or lost, and
- they can have integrated cameras, which can lead to child protection, bullying and data protection issues.

The School will not tolerate cyber-bullying against either pupils or staff. Sending inappropriate, suggestive or abusive messages is forbidden and anyone who is found to have sent a message, either in School or off site, of such content will be disciplined. For more information on the School's disciplinary sanctions read the School Behaviour and Discipline Policy.

The School's filtering systems prohibit the access of social media sites in School.

The School takes certain measures to ensure that mobile phones and other smart devices are used responsibly in School. Some of these are outlined below:

- Pupils in years 7, 8 & 9 are required to hand in their mobile phone or other smart device on arrival at School and place them into the respective form mobile phone box. Phones are returned to the pupils at the end of the School day;
- Pupils in years 10 & 11 are required to hand in their mobile phone or other smart device during morning registration. Phones are returned to them at the end of the School day;
- Year 7-11 pupils are required to seek permission from their **Form Tutor or the Pastoral Support Officer** if they wish to use their mobile phone during the School day. This should only occur infrequently in the knowledge and understanding that if pupils need to contact parents as an emergency during the School day, this can be done via the Pastoral Support Officer's phone and thus does not require the pupils having access to their personal phones and/or smart watches;
- Members of the Sixth Form are required to restrict their use of mobiles phones to the Sixth form area on the 4th floor **ONLY;**
- This means that phones and/or smart watches are not allowed to be visible in lessons, assemblies or whilst transiting around the School (*the exception to this is if the teacher has given pupils permission to use the mobile phones in lessons);*
- Mobile phones and/or smart watches can be confiscated by a member of staff, and the device can be searched by a member of the Senior Leadership Team following permission from the Head, if there is reason to believe that there may be evidence of harmful or inappropriate use on the device;
- Mobile phones must be switched off during School lessons or any other formal School activities;
- Any pupil who brings a mobile phone or personal device into School is agreeing that they are responsible for its safety. The School will not take responsibility for personal devices that have been lost, stolen, or damaged;
- Images or files should not be sent between mobile phones in School, and
- Smart watches are not permitted to be worn in school. They should be handed in along with other mobile devices each day.

Instances of alleged misuse of mobile phones or personal devices should be reported to the Deputy Head Pastoral.

## 13.1 Laptops and other BYOD/personal devices

The use of BYOD devices is governed by the same rules and guidelines as mobile phones with the following exceptions:

All pupils are required to bring a laptop to School. Year 7 students will purchase a Chromebook through the School's approved provider and this will be managed by the School.

## 13.2 Mobile phone, smart devices or other BYOD/personal device misuses

**Pupils**

- Pupils who breach School policy relating to the use of personal devices will be disciplined in line with the School's Behaviour and Discipline Policy and Anti-bullying Strategy. Their mobile phone and/or smart watch and/or BYOD may be confiscated, and
- **Pupils are under no circumstances allowed to bring mobile phones, smart watches or personal devices into examination rooms.** If a pupil is found with a mobile phone in their possession it will be confiscated. The breach of rules will be reported to the appropriate examining body and may result in the pupil being prohibited from taking that exam.

**Staff**

- Staff are to follow the Staff Code of Conduct at all times;
- Under no circumstances should staff use their own personal devices to contact pupils or parents either in or out of School time;
- Staff are not permitted to take photos or videos of pupils. If photos or videos are being taken as part of the School curriculum or for a professional capacity, the School equipment will be used for this;
- The School expects staff to lead by example. Use of personal mobile phones should be limited to the staff room or offices or other designated areas during School hours;
- Any breach of School policy may result in disciplinary action against that member of staff. More information on this can be found in the Safeguarding and Child protection Policy, or in the staff contract of employment, and
- Use of personal devices is included in the Employee Handbook under Computers and Electronic Communications.

## 13.3 Webcams and Video Conferencing

Webcams and video conferencing may be used on occasions to support learning but only under the direct supervision of a member of staff. Misuse of these technologies should be reported to the Deputy Head Pastoral and sanctions may be applied according to the Behaviour and Discipline Policy.

# 14. Training

All new staff members will receive training, as part of their induction, on safe internet use and 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 meetings).

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 messages;
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups, and
    - 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 up the risks;
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term;
- Be aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices, and
- Be aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation.

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.

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

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

# 15. Managing information systems

The School is responsible for reviewing and managing the security of the computers and internet networks as a whole and takes the protection of School data and personal protection of our School community very seriously. This means protecting the School network, as far as is practicably possible, against viruses, hackers and other external security threats. The security of the School information systems and users will be reviewed regularly by the IT technician and virus protection software will be updated regularly.

Some safeguards that the School takes to secure our computer systems are:

- Ensuring that all personal data sent over the internet or taken off site is encrypted, and
- Making sure that unapproved software is not downloaded to any School computers.

Administrative permissions are limited to the Senior Leadership Teams that prevent unauthorised downloads.

- Files held on the School network will be regularly checked for viruses;
- The use of user logins and passwords to access the School network will be enforced, and
- Portable media containing School data or programmes will not be taken off-site without specific permission from a member of the senior leadership team.

For more information on data protection in School please refer to our Data Protection Policy. More information on protecting personal data can be found in section 11 of this policy.

### 15.1 Parents and Pupils

Parents and Pupils should ensure that they have the Smoothwall security certificate installed on their BYOD to ensure their daughters are safe online in School.

## 16. Monitoring and Reviewing Online Safety

Technology and risks and harms related to it evolve and change rapidly. As such, we will conduct an annual review of our approach to online safety, supported by an annual risk assessment which includes a 360 safe online safety self-review tool to inform our policies and procedures.

In light of the responsibility to safeguard and promote the welfare of children and provide pupils with a safe environment in which to learn, the Governors will do all that they reasonably can, in keeping with their statutory duty, to limit our pupils' exposure to risks from the School's IT system. As part of this process, Governors will ensure that our filtering and monitoring systems are appropriate.

The appropriateness of our filtering and monitoring system is informed, in part, by the risk assessment required by the Prevent Duty. Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the Senior Leadership Team.

The Senior Leadership Team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.

All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard pupils; effective BYOD classroom management and regular education about safe and responsible use is essential.

More House currently uses Smoothwall to monitor the internet usage of pupils.

All Online behaviour concerns and safeguarding issues are logged on CPOMS.

## 17. Related Policies

This E-Safety policy is linked to our:

- Safeguarding and Child Protection Policy;
- Policy on Behaviour and Discipline;

- Anti-bullying Strategy;
- Privacy Notice;
- Employee Handbook;
- Relationships and Sex Education (RSE);
- PSHE Policy;
- Staff Disciplinary Policy and Procedures;
- Staff Code of Conduct, and
- Complaints procedures.

## Appendix 1: Acceptable use of BYOD, Internet, Emails and Computers and all Devices in School

MORE HOUSE SCHOOL
KNIGHTSBRIDGE

| ACCEPTABLE USE OF A LAPTOP OR THE SCHOOL'S ICT FACILITIES AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS |
|---|
| **Name of pupil:** |

At More House School we understand the importance and benefits of emerging technologies for pupil's learning and personal development. However, we also recognise that safeguards need to be in place to ensure pupils are kept safe at all times.

Please could parents read and discuss this policy with their child and then sign and return to the School office.

- I will only use ICT systems in School, including the BYOD, internet, email, digital video, mobile technologies, etc. for School purposes.
- I will not download or install software on School equipment. Equally I will not download or use any apps or software in lessons that the classroom teacher has not provided permission for.
- I will only log on to the School network/ learning platform with **my own** username and password. I understand that I am responsible for keeping this information secure.
- I will follow the School's ICT security system and not reveal my passwords to any other person. I will change my passwords regularly.
- I will only use my School email address
- I will only use Google Chrome as my web browser in School and I will ensure that I am logged into Google Chrome with my School email address at all times.
- I will make sure that all ICT communications with pupils, teachers or others is responsible, sensible, polite and courteous and such that upholds the dignity of each and every individual.
- I will be responsible for my behaviour when using the BYOD in lessons and accessing the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
- I will not give out any personal information such as name, phone number or address.

- I understand that images of pupils will only be taken, stored and used for School purposes in line with School policy and not be distributed outside the School network without parental permission.
- I will ensure that my online activity, both in School and outside School, will not cause my School, the staff, pupils or others distress or bring them into disrepute.
- I will support the School approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the School community or any other individual.
- I will respect the privacy and ownership of others' work online at all times. I realise that plagiarism of others' work is a serious disciplinary matter. Plagiarism is presenting someone else's work or ideas as your own, with or without their consent, by incorporating it into your work without full acknowledgement. Plagiarism may be intentional or reckless, or unintentional. Under the regulations for examinations, intentional or reckless plagiarism is a disciplinary offence.
- I will not attempt to bypass the internet filtering system including streaming internet networks from my mobile or smart technology.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers.
- I understand that these rules are designed to keep me safe and that if they are not followed, School sanctions will be applied and my parents may be contacted.

| | |
|---|---|
| Signed (pupil): | Date: |
| Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these. | |
| Signed (parent/carer): | Date: |

## Appendix 2: Acceptable use agreement (staff, governors and volunteers)

| Acceptable use of the school's ICT systems and internet: agreement for staff, governors and volunteers | |
|---|---|
| **Name of staff member/governor/volunteer:** | |
| **When using the school's ICT systems and accessing the internet in school, or outside school on a work device, I will not:**<br><br>• Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material);<br>• Use them in any way which could harm the school's reputation;<br>• Access social networking sites or chat rooms;<br>• Use any improper language when communicating online, including in emails or other messaging services;<br>• Install any unauthorised software, or connect unauthorised hardware or devices to the school's network;<br>• Share my password with others or log in to the school's network using someone else's details;<br>• (for volunteers) Take photographs of pupils without checking with teachers first<br>• Share confidential information about the school, its pupils or staff, or other members of the community;<br>• Access, modify or share data I am not authorised to access, modify or share, and<br>• Promote private businesses, unless that business is directly related to the school. | |
| • I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role;<br>• I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems;<br>• I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy;<br>• I will let the designated safeguarding lead (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, and<br>• I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.<br>• I will take appropriate care of any equipment provided to me by the school and will return the equipment to the IT technician on or before the last day of school before the contract termination date. | |
| Signed (staff member/governor/volunteer): | Date: |

## Appendix 3: Online safety training needs – Self-Audit for staff

MORE HOUSE SCHOOL
KNIGHTSBRIDGE

| Online safety training needs audit | |
|---|---|
| **Name of staff member/volunteer:** | **Date:** |
| **Question** | **Yes/No (add comments if necessary)** |
| Do you know the name of the person who has lead responsibility for online safety in school? | |
| Are you aware of the ways pupils can abuse their peers online? | |
| Do you know what you must do if a pupil approaches you with a concern or issue? | |
| Are you familiar with the School's acceptable use agreement for staff, volunteers, governors and visitors? | |
| Are you familiar with the School's acceptable use agreement for pupils and parents? | |
| Do you regularly change your password for accessing the school's ICT systems? | |
| Are you familiar with the School's approach to tackling cyber-bullying? | |
| Are there any areas of online safety in which you would like training/further training? | |