St Joseph's In The Park
Independent Prep School

St Joseph's in the Park

Online Safety Policy 2023

Contents

Introduction

This policy relates to St Joseph's in the Park School, which is one of the eight Mill Hill School Foundation ('the Foundation') schools.

1. The Foundation recognises that IT and the internet are fantastic tools for learning and communication that can be used in school to enhance the curriculum, challenge pupils, and support creativity and independence. Using IT to interact socially and share ideas can benefit everyone in the Foundation community, but it is important that the use of the Internet and IT is seen as a responsibility and that pupils, staff and parents use it appropriately and maintain good practice online. It is important that all members of the Foundation community are aware of the dangers of using the Internet and how they should conduct themselves online.

Online safety covers the Internet, but it also covers mobile phones and other electronic communications technologies. We know that some adults and young people may attempt to use these technologies to harm children. The harm might range from sending hurtful or abusive texts and Emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings.

There is a 'duty of care' for any persons working with children and educating all members of the Foundation community on the risks and responsibilities of online safety falls under this duty. It is important that there is a balance between controlling access to the Internet and technology and allowing freedom to explore and use these tools to their full potential. This policy aims to be an aid in regulating IT activity in the Foundation and provide a good understanding of appropriate IT use that members of the Foundation community can use as a reference for their conduct online both inside and outside of school hours.

Online safety is a whole-Foundation issue and responsibility.

This policy and our requirements for the acceptable use of IT within the Foundation cover both fixed and mobile internet devices provided by the Foundation (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.); as well as all devices owned by pupils and staff brought onto school/Foundation premises (personal laptops, tablets, wearable technology e.g. smart phones and watches, etc.). They also cover when pupils are going online in the home environment, for example when accessing remote learning.

Communicating Foundation Policy - This policy is available from the relevant School Office and is on the Foundation and the schools' websites for parents, staff, and pupils to access when and as they wish. Rules relating to the Foundation code of conduct when online, and online safety guidelines, are displayed around the Foundation. Online safety is integrated into the curriculum in any circumstance where the Internet or technology are being used, and during PSHE lessons where personal safety, responsibility, and/or development are being discussed.

The Foundation holds events for parents on Internet Safety and includes advice on Online Safety in its Safeguarding Bulletins which are circulated to Governors, parents and staff.

This policy should be read in conjunction with the following policies/guidance for further clarity:

- Safeguarding and Protecting the Welfare of Pupils Policy
- Anti-Bullying Policy
- Promoting Positive Behaviour Policy
- Staff Code of Conduct
- Personal, Social. Health and Economic Education (PSHEE) Policy
- Relationships and Sex Education (RSE) Policy
- Educational Visits Policy
- Data Protection Policy
- Whistleblowing Policy
- DfE Guidance on Teaching Online Safety in Schools (June 2019, updated Jan 2023)
- Keeping Children Safe in Education 2023 (KCSIE)
- UKCIS Education for a Connected World Framework (June 2020)
- DfE Advice on Sharing nudes and semi-nudes, advice for education settings 2020
- Early Years Foundation Stage 2023
- Hertfordshire Safeguarding Children Partnership Procedures

Making use of IT and the Internet in the Foundation

2.

The internet is used in the Foundation schools to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the Foundation's management functions. Technology is advancing rapidly and is now a huge part of everyday life, education and business. We want to equip our pupils with all the necessary IT skills that they will need to enable them to progress confidently into a professional working environment when they leave school. However, we also need to prepare the pupils for the more subtle risks that go hand in hand with technology. Our pupils are therefore not just taught to use the internet and information communication technology, but how to stay safe in the online

3. environment and how to mitigate risks.

Importance

The Foundation acknowledges the provisions of KCSIE which states: 'Technology is a significant component in many safeguarding and wellbeing issues'. Children are at risk of abuse online as well as face to face. In many cases abuse will take place concurrently via online channels and in daily life. Technology can often provide a platform which facilitates: child sexual exploitation, radicalisation, and sexual predation: An effective approach to online safety therefore empowers a school to protect and educate the whole school community in their use of technology and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate.

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful material, for example pornography, fake news, racist or radical and extremist views

- **Contact**: being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults, and
- **Conduct**: personal online behaviour that increases the likelihood of, or causes, harm: for example making, sending and receiving explicit images, or online bullying
- **Commerce**: being exposed to risks such as online gambling, inappropriate advertising, phishing and or financial scams

Responsibilities

4. The Foundation Online Safety Coordinators: These are the Designated Safeguarding Leads (DSL) for each Foundation School as they have responsibility for online safety, including online filtering and monitoring in their school.

At St Joseph's, the DSL is Mrs Nicole Welsh, Assistant Head (Teaching and Learning).

The Foundation IT Director is Mr Firas Al-Fakhri, and the designated member of the governing body responsible for online safety is Mr Nigel Taylor (Governor Responsible for Safeguarding).

The Director of Safeguarding for the Foundation is Mrs Jane Morris. She can be contacted at: Jane.morris@mhsfoundation.uk.

4.1 Governors

In line with KCSIE 2023, the Court of Governors holds online safety as a central theme in their whole-setting approach to safeguarding. It is essential that pupils are safeguarded from potentially harmful and inappropriate online material. Their approach to online safety empowers the Foundation to protect and educate pupils and staff in their use of technology, with mechanisms in place to identify, intervene in, and escalate any concerns where appropriate.

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy by reviewing online incidents and monitoring reports. Online safety falls within the remit of the Governor responsible for Safeguarding.

The role of the Online Safety Governor will include:

- ensuring an online safety policy is in place, reviewed every year and/or in response to an incident and is available to all stakeholders
- ensuring that each school has a DSL with responsibility for online safety who has been trained to a higher level of knowledge which is relevant to the school, up to date and progressive
- ensuring that safeguarding training for staff, including online safety training, is integrated and considered as part of the whole school safeguarding approach
- ensuring that pupils are taught about safeguarding, including online safety
- ensuring that procedures for the safe use of IT and the Internet, including appropriate online filters and monitoring systems, are in place and adhered to
- holding the Head for each Foundation school and staff accountable for online safety

4.2 Head and Senior Leadership Team

The Head of each Foundation school has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the DSL who has been appointed Online Safety Coordinator. Any complaint about staff misuse of technology by school staff must be referred to the Head as a safeguarding issue involving a member of staff.

The role of the Head will include:

- Ensuring access to induction and training in online safety practices for all users
- Ensuring all staff receive regular, up to date training
- Ensuring appropriate action is taken in all cases of misuse
- Working with the Foundation IT Director to ensure that Internet filtering methods are appropriate, effective and reasonable
- Ensuring that pupil or staff personal data as recorded within school management system sent over the Internet is secured
- Working in partnership with the Department for Education (DfE), the Internet Service Provider and Foundation IT Director to ensure systems to protect pupils are appropriate and managed correctly
- Working with the Foundation IT Director to ensure the Foundation IT system is reviewed regularly regarding security and that virus protection is installed and updated regularly
- The DSL will receive monitoring reports detailing matters for concern and/or investigation and will share these with the SLT as appropriate.

4.3 Designated Safeguarding Lead of each Foundation School

The DSL is acknowledged as having overall responsibility for online safeguarding within each school, including online filtering and monitoring. The DSLs and leadership teams follow the guidance regarding online safety within 'Keeping Children Safe in Education' 2023; and the DfE guidance outlining how schools can ensure their pupils understand how to stay safe and behave online as part of existing curriculum requirements.

Their role includes:

- Being able to understand the unique risks associated with online safety, including the additional risks that pupils with SEND face
- Leading online safety meetings
- Liaising with staff (especially pastoral support staff, school nurses, IT and SENDCOs) on matters of safety and safeguarding, including online and digital safety
- Working in partnership with the DfE and the Internet Service Provider and Foundation IT Manager to ensure systems to protect pupils are reviewed and improved
- Receiving reports of online safety incidents and creating a log of incidents to inform future online safety developments
- Reporting to Senior Management Team/Head of their School
- Liaising with the nominated member of the governing body & their Head to provide an annual report on online safety
- Co-ordinating the training and workshops for pupils, staff, Governors and parents to improve understanding of all aspects of online safety

- Keeping up to date on current online safety issues and guidance issued by relevant organisations, including the ISI, the Local Authority, CEOP (Child Exploitation and Online Protection), Childnet International, NSPCC, and the LSCP for Herfordshire.

4.4 IT Director/Technical Staff

The Foundation IT Director is responsible for ensuring

- That the Foundation's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the Foundation meets required online safety technical requirements and any relevant body online safety policy/guidance that may apply
- The Foundation IT Director is invited to DSL meetings on a termly basis
- That users may only access the networks and devices through a properly enforced password protection policy
  This Online Safety Policy, together with the School's approach to filtering and monitoring is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person
- That they keep up to date with online safety technical information to effectively carry out their online safety role and to inform and update others as relevant
- That the use of the network/internet/Virtual Learning Environment/remote access/Email is regularly monitored in order that any misuse/attempted misuse can be reported to the Head of the relevant school or the Director of Finance and Resources or the DSL for investigation/action/sanction
- That monitoring software/systems are implemented and updated as agreed in Foundation policies.
- Ensure the Foundation's IT system is reviewed regularly with regard to security and that virus protection is installed and updated regularly

4.5 Foundation Staff

Foundation staff are expected to:

- Read and follow the provisions of this Policy
- Read and Agree to the Acceptable Use of IT Policy/Agreement (Staff and Governors)
- Attend training sessions organised by the Foundation to promote online safety
- As with all issues of safety, staff are encouraged to create a talking and listening culture, in order to address any online safety issues which may arise in classrooms on a daily basis.
- Report to the DSL of their School (in respect of pupils) or the Head of their School (in respect of other members of staff) if they become aware of misuse or attempted misuse of Digital Technology within the Foundation

4.6 Pupils

Pupils are expected to:

- Read and agree to the Foundation's Acceptable Use of IT Agreement (Pupils) relating to the use of digital technology and accessing the Foundation Wi- fi
- Exercise their responsibility to speak out when they believe that the school's systems are being abused in any way

4.7 Parents

The school believes that it is essential for parents, guardians and carers to be fully involved with promoting online safety both in and outside of school. We regularly consult and discuss online safety with parents, guardians and carers to reinforce the importance of children being safe online.

It is important for parents and carers to be aware of what their children are being asked to do online, including the sites the school will ask them to access and who they will be asked to interact with online.
They are therefore advised to:

- Read Foundation Online Safety Guidance for parents that is circulated from time to time
- Attend Online Safety sessions and training sessions organised by the Foundation

Education and training

5.1 Staff: awareness and training

5.

- New teaching staff receive information on online safety and acceptable use as part of their induction.
- All teaching staff receive regular information and training on online safety issues in the form of targeted training and internal briefings, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of online safety. This includes updated information regarding online filtering and monitoring responsibilities and procedures in the school.
- Staff training in the School is logged centrally.
- All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school online safety procedures. When children use school computers, staff should make sure children are fully aware of the agreement they are making to follow the school's acceptable use guidelines.
- Teaching staff are encouraged to incorporate online safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the school community.
- All incidents relating to online safety should be reported to the DSL.

5.2 Pupils: Online safety in the curriculum

The Foundation delivers age, and stage of development-, appropriate online education through the tutor programme, PSHE, assemblies, discussion, talks and the academic curriculum. These are planned and delivered using the guidance from the UKCIS outlined in the 'Education for a Connected World' framework:https://www.gov.uk/government/publications/education-for-a-connected-world.
This education aims to ensure that all pupils develop the underpinning knowledge and behaviours needed to navigate the online world safely, in a way which suits their age and ability. Teaching staff help pupils achieve this by reinforcing the Foundation's fundamental values, with a particular focus on being kind.

The through-Foundation curriculum focuses on the following:

- IT and online resources are used increasingly across the curriculum. We believe it is essential for online safety guidance to be given to pupils on a regular and meaningful basis. We continually look for new opportunities to promote online safety and regularly monitor and assess our pupils' understanding of it.
- The school provides opportunities to teach about online safety within a range of curriculum areas (as above), IT lessons, as well as informally when opportunities arise.
- At age-appropriate (and stage-of-development-appropriate) levels, and usually via PSHEE, pupils are taught to look after their own online safety.
- Enable pupils to understand what acceptable and unacceptable online behaviour looks like
- Raise awareness of the possible online risks and help pupils make informed decisions about how to act and respond
- Reinforce to all pupils the importance of knowing how, when and where they can seek support if they are concerned or upset by something they see or experience online
- Provide opportunities for pupils, parents and staff to have access to educational workshops, lectures and resources on the all aspects of online e- safety
- Recognise the consequences of inappropriate online behaviour in line with the Foundation's 'Pupil Behaviour Policy' but also on their own digital footprint
- Supporting pupils to understand and follow this Policy and the pupil guidance which may be issued by each School regarding the acceptable use of digital technology and online safety
- Again at age-appropriate points, pupils are taught about recognising online sexual exploitation, stalking and grooming, the risks, and of their duty to report any such instances they or their peers come across. Pupils can report concerns to the DSL (who is the Online Safety Lead) and indeed any member of staff at the school.
- Pupils are also taught about relevant laws applicable to using the internet; such as data protection and intellectual property. Pupils are taught about respecting other people's information and images.
- Pupils should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the school's Anti-bullying Policy, which describes the preventative measures and the procedures that will be followed when the school discovers cases of bullying). Pupils should approach the DSL who is the school's Online Safety Lead or other member of staff as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies.

5.3 Pupils: Vulnerable Pupils

- The school is aware that some pupils are considered to be more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.
- The school will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable pupils.
- The school will seek input from specialist staff as appropriate, including the SENCO.

Cyberbullying

6. The Foundation, as with any other form of bullying, takes cyber bullying, very seriously. Information about specific strategies or programmes in place to prevent and tackle bullying is set out in each Foundation school's Pupil Promoting Positive Behaviour policy and its Anti-Bullying Policy. The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to members of the Foundation community 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.

If an allegation of bullying does come up, the Foundation will:

- Take it seriously
- Act as quickly as possible to establish the facts. It may be necessary to examine Foundation systems and logs or contact the service provider to identify the bully
- Record and report the incident
- Provide support and reassurance to the victim and support the perpetrator via the individual School's Promoting Positive Behaviour Policy

The Threat of Online Radicalisation

7. The internet and the use of social media in particular has become a major way to communicate with others, especially young people, which has provided access for like-minded people to create an online community and confirm extreme beliefs such as extreme ideological views or the use of violence to solve problems.

In line with Prevent guidance, protecting children from the risk of radicalisation, the Foundation has a number of measures in place to ensure that children are safe from terrorist and extremist material when accessing the internet in school, and to help prevent the use of social media for this purpose:

- Web site filtering and monitoring is in place to help prevent access to terrorist and extremist material and social networking sites such as Facebook, Instagram or Twitter by pupils
- Pupils, parents and staff are educated in safe use of social media and the risks posed by on-line activity, including from extremist and terrorist groups.
- Further details on how social media is used to promote extremism and radicalisation can be found on the Educate Against Hate website (www.educateagainsthate.com), which is designed to equip schools and college leaders, teachers and parents with the information, tools and resources they need to recognise and address extremism and radicalisation in young people, including in online issues.

Responding to Online Safety Incidents and Concerns

8. All members of the school community will be made aware of the reporting procedure for online safety and safeguarding concerns regarding pupil welfare, including breaches of filtering, youth produced sexual imagery (sexting), upskirting, cyberbullying, sexual harassment and illegal content. The school requires staff, parents, carers and pupils to work in partnership to resolve online safety issues.

All members of the community must respect confidentiality and the need to follow the official school procedures for reporting concerns. For further detailed information, the school Safeguarding and Protecting the Welfare of Pupils Policy, Complaints Policy and Procedures, and Whistleblowing Policy can be found on the school website.

After any investigations are completed, the school will debrief, identify lessons learnt and implement any policy or curriculum changes as required.

If the school is unsure how to proceed with an incident or concern, the DSL will seek advice from the Local Authority Safeguarding Team. Where there is suspicion that illegal activity has taken place, the school will contact the Local Authority Safeguarding Team or the Police using 101, or 999 if there is immediate danger or risk of harm.

Any allegations regarding a member of staff's online conduct will be referred to the Head and discussed with the DSL/Online Safety Lead and the LADO (Local Authority Designated Officer) if necessary. Appropriate action will be taken in accordance with the Staff Code of Conduct.
When made aware of concerns involving consensual and non-consensual sharing of nudes and semi-nude images and/or videos by children, staff are advised to:

- Report any concerns to the DSL immediately.
- Never view, copy, print, share, store or save the imagery, or ask a child to share or download it – this may be illegal. If staff have already viewed the imagery by accident, this will be immediately reported to the DSL.
- Not delete the imagery or ask the child to delete it.
- Not say or do anything to blame or shame any children involved.
- Explain to child(ren) involved that they will report the issue to the DSL and reassure them that they will receive appropriate support and help.
- Not ask the child or children involved in the incident to disclose information regarding the imagery and not share information about the incident with other members of staff, the child(ren) involved or their, or other, parents and/or carers. This is the responsibility of the DSL.

The DSL will respond to the concerns as set out in the non-statutory UKCIS guidance: Sharing nudes and semi-nudes: advice for education settings working with children and young people - GOV.UK (www.gov.uk)

For further details regarding the procedures for responding to specific online incidents or concerns, please contact the DSL/Online Safety Lead.

Monitoring and Filtering

9. The Foundation will ensure that appropriate filtering and monitoring systems are in place when pupils and staff access school systems and internet provision, so that exposure to any risks can be reasonably limited. Filtering and monitoring are both important parts of safeguarding pupils and staff from potentially harmful and inappropriate online material, but without unreasonably impacting teaching and learning, in line with the DfE filtering and monitoring standards which were updated in March 2023.

We review our approach to filtering and monitoring regularly and assess the effectiveness of the current provision, any gaps, and the specific safeguarding needs of pupils (their age ranges, those who are at greater risk of harm for example those with SEND, or those with English as an Additional Language (EAL)) and staff. This happens annually (at the very least), or more often if circumstances dictate, such as when:

- a safeguarding risk is identified
- there is a change in working practice, like remote access or BYOD
- new technology is introduced

Any checks to the Foundation's filtering provision are completed and recorded as part of the filtering and monitoring review process. The Governors have overall strategic responsibility for meeting this requirement, and they have assigned day to day responsibility for the following to the Governor with specific responsibility for IT, the Heads and the Foundation IT Director:

- procuring filtering and monitoring systems
- reviewing the effectiveness of the Foundation's provision
- overseeing reports

They must also ensure that all staff:

- are appropriately trained for their role
- understand that it is everyone's responsibility to keep the online environment safe, including the effective use of filtering and monitoring
- follow the Staff Code of Conduct, all policies, processes and procedures
- act on reports and concerns, and record them appropriately

The DSL has the lead responsibility for safeguarding and online safety, which includes overseeing and acting on:

- filtering and monitoring reports
- safeguarding concerns
- checks to filtering and monitoring systems

The IT Support Department has the technical responsibility for:

- maintaining filtering and monitoring systems
- providing filtering and monitoring reports
- completing actions following concerns or checks to systems

It is important to be able to identify individuals who might be trying to access unsuitable or illegal material so they can be supported by appropriate staff, such as the senior leadership team or the designated safeguarding lead.

The Foundation therefore reserves the right to regularly monitor and filter an employee's/pupil's use of the internet, social media and e-mail systems when at work or when using Foundation electronic equipment. Such monitoring/filtering includes the right to read e-mails sent or received on electronic equipment provided by the Foundation or view photographic images captured on electronic equipment provided by the Foundation to check that the use by employees is in accordance with this policy.

All staff need to be aware of reporting mechanisms for safeguarding and technical concerns. They must report if:

- they witness or suspect unsuitable material has been accessed
- they can access unsuitable material
- they are teaching topics which could create unusual activity on the filtering logs
- there is failure in the software or abuse of the system
- there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks
- they notice abbreviations or misspellings that allow access to restricted material

The Court of Governors support the Senior Leadership Team to review the effectiveness of monitoring strategies and reporting process. Any incidents that are picked up, are acted on with urgency and outcomes are recorded. Incidents could be of a malicious, technical, or safeguarding nature. Staff know that in the first instance, they report their concerns to the DSL.

There is a Foundation Information Governance Group that meets three times a year, comprising IT (Chair), Safeguarding, Compliance and Data Protection to discuss all safeguarding related technology, security, incidents, issues and concerns, policy reviews etc. Findings are reported back to Governors as required.

10. If it is discovered that any of the systems are being abused and/or that the terms of this Policy are being infringed, disciplinary action may be taken in accordance with the provisions of the Foundation's disciplinary policies and procedures.

Online Safety Review

The DSL of each Foundation School will regularly review its Online Safety Provision and Education as part of the annual Safeguarding Audit.

Security and Management of Information Systems

The Foundation takes the protection of Foundation data and personal protection of our Foundation community very seriously. This means protecting the Foundation network, as far as is practicably possible, against viruses, hackers and other external security threats. The
11. Foundation IT Director will review the security of the Foundation information systems and users regularly and virus protection software will be updated regularly at least annually (or more regularly if circumstances dictate).

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

- Advising staff that all personal data sent over the Internet or taken off site should be encrypted
- Making sure that unapproved software/apps are not downloaded to any Foundation devices. Alerts will be set up to warn users of this.
- Files held on the Foundation network will be regularly checked for viruses
- The use of secure user logins and passwords to access the Foundation network will be enforced
- Portable media containing school data or programmes will not be taken off-siteAny security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT will be immediately reported to the IT team.

For more information on data protection in the Foundation please refer to theData Protection Policy.

12.

Emails

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

- Initiating contact and projects with other schools nationally and internationally
- Providing immediate feedback on work, and requests for support where it is needed

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

12.1 Staff Use of Email

Staff should be aware of the following when using emails in the Foundation:

- Staff should only use official Foundation-provided email accounts to communicate with pupils, parents or carers. Personal Email accounts should not be used to contact any of these people.
- The Foundation permits the incidental personal use of email, the internet, social media and related types of electronic communication and information, and electronic equipment by an employee as long as it is kept to a minimum and takes place substantially out of normal working hours.
- Staff should be aware that all their personal interactions (email and internet) on a Foundation device are logged, and may be monitored.
- Use must not interfere with an employee's work commitments, or those of others. If it is discovered that excessive periods of time have been spent on the internet or other electronic media provided by the Foundation, either in, or outside, working hours disciplinary action may be taken and internet access or use of electronic equipment may be withdrawn without notice at the discretion of the Head or the Director of Finance and Resources (DFO) or Chief Executive Officer (CEO) of the Foundation.
- Emails sent from Foundation accounts should be professionally and carefully written. Staff are always representing the Foundation and should take this into account when entering into any email communications.
- Where possible, staff should avoid 'replying to all' or blindly forwarding emails they have received. Be selective in your email use.
- 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 the Foundation
- Using photographic material of any kind to bully, harass or intimidate others will not be permitted and will constitute a serious breach of discipline and may lead to dismissal

12.2 Pupil Use of Email

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

- In school, pupils should only use Foundation-approved email accounts
- 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
- 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 PSHE curriculum to identify spam, phishing and virus emails and attachments that could cause harm to the Foundation network or their personal account or wellbeing.

Safe Use of Digital and Video Images of Pupils

13. 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, guardians or carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff will 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).

13.1 The School's Website

The Foundation considers the school's website to be a useful tool for communicating our ethos and practice to the wider community. It is also a valuable resource for parents, pupils, and staff for keeping up- to-date with Foundation news and events, celebrating Foundation wide achievements and personal achievements, and promoting school projects.

Any information published on the website will comply with good practice guidance on the use of such images, and be carefully considered in terms of safety for the Foundation community, copyrights and privacy policies. No personal information on staff or pupils will be published, and details for contacting the Foundation will be for the relevant school office only.

13.2 Safe Use of Pupil Digital Images and Data

Under the Data Protection Act 2018 images of pupils and staff will not be displayed in public, either in print or online, without consent. On admission to each Foundation school parents/carers will be asked to sign a photography consent form. For pupils 13 and above their explicit consent is also required. The Foundation does this to prevent repeatedly asking parents for consent over the school year, which is time-consuming for both parents and the Foundation. The terms of use of photographs never change, and so consenting to the use of photographs of your child over a period rather than a one-off incident does not affect what you are consenting to.

Published images do not identify pupils or put them at risk of being identified unless they or their parents/carers consent except that pupils may be identified by their first name only.

Images published on the website cannot be reused or manipulated. Only images created by or for the school/Foundation will be used in public and pupils may not be approached or photographed while in school or doing school activities without the Foundation/school's permission.

The Foundation follows general rules on the use of photographs/videos of pupils.

13.2.1 By Parents

At St Joseph's, parents are not permitted to take photographs or use their mobile phones at any time around the School other than at specific events when express permission has been given.

13.2.2 By the Foundation

- At the Foundation we want to celebrate the achievements of our pupils and therefore may want to use images and videos of our pupils within promotional materials, or for publication in the media such as local, or even national, newspapers covering school events or achievements. We will seek the consent of pupils, and their parents where appropriate, before allowing the use of images or videos of pupils for such purposes
- Whenever a pupil begins their attendance at a Foundation School, they, or their parent where appropriate, will be asked to complete a consent form in relation to the use of images and videos of that pupil. We will not use images or videos of pupils for any purpose where we do not have consent
- At St Joseph's, teachers use the EYFS Online Learning Journal on Tapestry, which allows for parental access. Parents may not share photos from this forum. Please refer to the school for more information about obtaining the images. Please refer to the Appendix 3 for more details
- Staff and volunteers are allowed to take digital and video images to support educational aims, but must follow this policy concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment: personal equipment should not be used for such purposes.

13.3 Complaints regarding the Misuse of Digital Images or Video

Parents should follow the standard school complaints procedure if they have a concern or complaint regarding the misuse of photographs/images/videos published by the school. Please refer to our Concerns and Complaints Policy. Any issues or sanctions will be dealt with in line with the school's Safeguarding and Protecting the Welfare of Pupils Policy.

Misuse of images/videos in any form by pupils and others, will be dealt with in accordance with the school's Promoting Positive Behaviour Policy and the Anti-bullying Policy according to the type of incident. Should there be a case of pupils sharing nudes and semi-nudes of under-18s, which is illegal even with the individual's consent, the matter will be immediately referred to the DSL and the Head.

14.

Social Media, Social Networking and Personal Publishing

Personal publishing tools include blogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging. These online forums are the more obvious sources of inappropriate and harmful behaviour and where pupils are potentially more vulnerable to content, contact and conduct behavioural issues. Pupils at St Joseph's are prohibited from using these sites while on the school grounds or an educational visit/residential trip.

14.1 Expectations

- The expectations' regarding positive, safe and responsible use of social media applies to all members of the Foundation community. The school will control pupil and staff access to social media whilst using school provided devices and systems on site.
- All members of the Foundation community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- Concerns regarding the online conduct of any member of the Foundation community on social media, should be reported to the Head and will be managed in accordance with our Anti-Bullying, Behaviour, and Safeguarding Policies, and Staff Code of Conduct.

14.2 Staff Personal Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities. Further guidelines are found in the Staff Code of Conduct.

14.3 Pupils' Personal Use of Social Media

- Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive education approach, via age appropriate sites and resources.
- Pupils are expected not to engage in threatening, hurtful or defamatory online behaviour on social media platforms, in interactive online games or in the metaverse.

14.4 Official School Use of Social Media

- The official use of social media sites, by the school, only takes place with clear educational or community engagement objectives, with specific intended outcomes.
- Official school social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only. Official social media sites are suitably protected and, where possible, run and/or linked to/from the school website.
- Official social media use will be conducted in line with existing policies, including: Anti-Bullying, Data Protection, Safeguarding and the Staff Code of Conduct.

15.

Use of Foundation and Personal Mobile Phones and Devices

While mobile phones and personal communication devices are commonplace today, their use and the responsibility for using them should not be taken lightly. Some issues surrounding the possession of these devices are they:

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

15.1 Use by Staff

- Staff members must at all times act in the best interests of children and young people when creating, participating in or contributing content to social media sites.
- School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. Staff should only use the school device which is allocated to them for school work. When they are not using a device staff should ensure that it is locked to prevent unauthorised access.
- The school devices/cameras may be used for official photographs under the direction of the Head. These photographs must only be downloaded using the school's computers and not onto a personal, private computer. Please refer to the Staff Code of Conduct for further details.
- Under no circumstances may staff contact a pupil or parent, guardian or carer using a personal telephone number, email address, social media or messaging system.
- Personal cameras belonging to staff and volunteers are not to be used on the school premises or school grounds at any time. Cameras on staff owned mobile phones should not be used on school premises or school grounds at any time. No images may be taken of the school or any pupils using mobile phones or personal cameras.
- Personal mobile phones may be used in dedicated staff areas or in class and teaching rooms only if the children are not present, or in the event of needing to use the authenticator application.
- Computing devices and wearables connected to the school network must always use updated software to safeguard against critical zero-day security vulnerabilities.
- Staff should not accept mobile phone calls during a lesson or when they are with children. The only exception to this is if the Head calls a staff member (usually only on Sports Days or on school trips, or if the School Office calls in similar circumstances). These calls will only be made in unusual or emergency situations.
- Staff are advised to ensure that Bluetooth or other forms of communication, such as 'airdrop', are hidden or disabled during lesson times.
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.
- The Foundation accepts no responsibility for, nor provides insurance against, theft, loss or damage of any employee's personal property, including electronic equipment. All such equipment is brought onto the Foundation site at the owner's risk.

15.2 Use by Pupils

- The Foundation has clear policies (age dependant) on the use of mobile and smart technology, reflecting the fact many children now have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access increases the risk that some children, whilst at school, are able to sexually harass, bully, and control others via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups), and view and share pornography and other harmful content.
- Pupils are not permitted to bring in/use mobile phones or other digital devices at St Joseph's and school staff are not permitted to use their own mobile phones or other digital devices whilst at school in line with the provisions of EYFS regulations
- If a pupil needs to contact their parents or carers whilst on site, they will be allowed to use a school phone – following permission from a teacher.

- Parents are advised to contact their child via the school office.

Management of Applications which Record Children's Progress (Data and Images)

16. The school uses applications such as Engage SMIS (Double First Ltd) Tapestry (EYFS), Google Classroom & Atom to track pupils progress and share appropriate information with parents and carers (this list is not exhaustive). The Head is ultimately responsible for the security of any data or images held of children. As such, they will ensure that tracking systems are appropriately risk assessed prior to use, and that they are used in accordance with GDPR and data protection legislation

To safeguard data:

- only school issued devices will be used for apps that record and store children's personal details, attainment or photographs.
- personal staff mobile phones or devices will not be used to access or upload content.
- school devices will be appropriately encrypted if taken off site to reduce the risk of a data security breach in the event of loss or theft.
- all users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
- parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

17.

Managing Emerging Technologies

Technology is progressing rapidly, and with the introduction of Artificial Intelligence (AI), new technologies are constantly emerging. The Foundation assesses the potential risks of any new technologies before permitting their use in schools, carefully weighing these up with the potential educational advantages they may offer. The Foundation may inject AI into their practices, and by doing so, stays at the forefront of innovation, proactively monitoring and keeping abreast of emerging technologies. This approach allows the Foundation to promptly devise and implement suitable strategies to navigate the ever-changing technological landscape.

18.

Protecting Personal Data

19. The Foundation takes its compliance with the Data Protection Act 2018 seriously. Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations (GDPR) and Data Protection legislation. Full information can be found in the Foundation's Data Protection Policy (available on the Foundation and school websites).

Breaches of Policy by Employees

Staff should refer to the Foundation's Staff Code of Conduct which sets out the full expectations for staff regarding Online Safety and Internet Use, and the Acceptable Use of IT Policy/Agreement. It details the repercussions that may follow if these standards are not followed.

A breach of this policy may be treated as misconduct and as such will be dealt with in accordance with the Foundation's Disciplinary policies and procedures. The Foundation reserves the right to contact the Police or other outside agency, as appropriate.

Where an employee wishes to complain about email, internet, social media, electronic images or related electronic communication, or electronic equipment use by another member of staff, they should inform the Head of the relevant School or if the matter involves a member of the Foundation Finance, Administration and Support Staff they should inform the Director of Finance and Resources and/or the Director of Operations. A complaint by an employee will be dealt with in a timely and appropriate manner in accordance with the provisions of the Foundation's Whistleblowing Policy.

If a complaint against an employee is made by a pupil or parent concerning a breach of this policy the matter will be dealt with in accordance with the Foundation's Concerns and Complaints Policy received from Parents.

If a breach of this policy raises a safeguarding concern the matter will be dealt with in accordance with the Foundation's Safeguarding and Protecting the Welfare of Pupils.

20. **Visitors' Use of Mobile and Smart Technology**

The school operates a no mobile phone/smart technology policy for all Visitors to the site. This is communicated to them when they sign in at reception.

21.
- Members of staff are expected to challenge visitors if they have concerns about their use of mobile and smart technology and will inform the DSL or IT Services Manager of any breaches of our policy.

Complaints

22. As with all issues of safety in school, if a member of staff, a pupil or a parent, guardian or carer has a complaint or concern relating to online safety, prompt action will be taken to deal with it. Complaints should be addressed to the DSL in the first instance, who will undertake an immediate investigation and liaise with the Leadership Team and any members of staff or pupils involved. Please see the Foundation Complaints Procedure for further information.

Review

This Policy is reviewed and updated annually, by the Foundation Executives and Pastoral Committee of the Court of Governors.

This Policy was approved by the Pastoral Committee of the Court of Governors on 19th Sept 2023

Review Date for Policy: September 2024

APPENDIX 1: St Joseph's Online Learning Tools in EYFS

Tapestry- Online Learning Journal EYFS

In Early Years at St Joseph's the secure online learning journal Tapestry is used to record observations and make assessments of children's learning. This allows staff and parents to access the information via a personal password protected login. Each child is allocated a class however all staff are able to capture observations for each other's children. Parents logging into the system are only able to see their child(ren)'s learning journal. Parent access allows them to comment (or 'reply') to observations that staff have inputted as well as adding their own observations and photos/videos. Before parents are linked to their child(ren)'s learning journal they are asked to give permission for their child's photo to appear in other children's learning journals. Before beginning to access the system, parents have to sign to agree not to download and share any information on any other online platforms or social networking sites (such as Facebook)

Safe Use Agreement

- Staff and parents should not share log in or password details with any person
- Staff should not share any information or photographs relating to children with any person not employed by Mill Hill Foundation
- Staff should take all responsible steps to ensure the safe keeping of any portable device e.g. iPad that they are using and report any missing devices
- If accessing Tapestry with a private computer, not on Foundation premises, staff must maintain confidentiality and professionalism
- All entries on Tapestry must be appropriate
- All entries on Tapestry remain the property of the Foundation
- At all times staff must comply with the Foundation's Child Protection policies

Google Classroom is used for years 1-6 and Atom is used for years 3-6 at St Joseph's In The Park. The same guidance and Safe Use Agreement, as above, also applies to these learning platforms.

APPENDIX 2: Sources of Information for schools and parents to keep children safe online

(The following list is not exhaustive but should provide a useful starting point).

There is a wealth of information available to support schools and parents/carers to keep children safe online. The following list is not exhaustive but should provide a useful starting point:

Advice for governing bodies/proprietors and senior leaders

- Childnet provide guidance for schools on cyberbullying
- Educateagainsthate provides practical advice and support on protecting children from extremism and radicalisation
- London Grid for Learning provides advice on all aspects of a school or college's online safety arrangements
- NSPCC provides advice on all aspects of a school or college's online safety arrangements
- Safer recruitment consortium "guidance for safe working practice", which may help ensure that the Staff Coode of Conduct and behaviour policies are robust and effective
- Searching screening and confiscation is departmental advice for schools on searching children and confiscating items such as mobile phones
- South West Grid for Learning provides advice on all aspects of a school or college's online safety arrangements
- Use of social media for online radicalisation - A briefing note for schools on how social media is used to encourage travel to Syria and Iraq
- UK Council for Internet Safety have provided advice on, and an Online Safety Audit Tool to help mentors of trainee teachers and newly qualified teachers induct mentees and provide ongoing support, development and monitoring
- Department for Digital, Culture, Media & Sport (DCMS) Online safety guidance if you own or manage an online platform provides practical steps on how companies can embed safety into the design of their online platforms. It offers information on common platform features and functions (such as private messaging) and their risks, as well as steps that can be taken to manage that risk.
- Department for Digital, Culture, Media & Sport (DCMS) A business guide for protecting children on your online platform provides guidance to businesses on how to protect children on their online platform. It outlines existing regulatory requirements and provides best practice advice on how to protect children's personal data, ensure content is appropriate for the age of users, ensure positive user-to-user interactions and address child sexual exploitation and abuse.

Support for children

- Childline for free and confidential advice
- UK Safer Internet Centre to report and remove harmful online content
- CEOP for advice on making a report about online abuse
- Parental support

- Childnet offers a toolkit to support parents and carers of children of any age to start discussions about their online life, to set boundaries around online behaviour and technology use, and to find out where to get more help and support
- Commonsensemedia provide independent reviews, age ratings, & other information about all types of media for children and their parents
- Government advice about protecting children from specific online harms such as child sexual abuse, sexting, and cyberbullying
- Government advice about security and privacy settings, blocking unsuitable content, and parental controls
- How Can I Help My Child? Marie Collins Foundation – Sexual Abuse Online
- Internet Matters provide age-specific online safety checklists, guides on how to set parental controls on a range of devices, and a host of practical tips to help children get the most out of their digital worldLet's Talk About It provides advice for parents and carers to keep children safe from online radicalisation
- London Grid for Learning provides support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online
- Stopitnow resource from The Lucy Faithfull Foundation can be used by parents and carers who are concerned about someone's behaviour, including children who may be displaying concerning sexual behaviour (not just about online)
- National Crime Agency/CEOP Thinkuknow provides support for parents and carers to keep their children safe online
- Net-aware provides support for parents and carers from the NSPCC and O2, including a guide to social networks, apps and games
- Parentzone provides help for parents and carers on how to keep their children safe online
- Parent info from Parentzone and the National Crime Agency provides support and guidance for parents from leading experts and organisations
- Talking to your child about online sexual harassment: A guide for parents – This is the Children's Commissioner's parent guide on talking to your children about online sexual harassment
- #Ask the awkward – Child Exploitation and Online Protection Centre guidance to parents to talk to their children about online relationships
- UK Safer Internet Centre provide tips, advice, guides and other resources to help keep children safe online

Remote education, virtual lessons and live streaming

- Case studies on remote education practice are available for schools to learn from each other
- Departmental guidance on safeguarding and remote education including planning remote education strategies and teaching remotely
- Guidance Get help with remote education resources and support for teachers and school leaders on educating pupils and students
- London Grid for Learning guidance, including platform specific advice
- National cyber security centre guidance on choosing, configuring and deploying video conferencing