St. Joseph's Catholic Primary School

Mater Christi Multi Academy Trust

Loving, Living, Learning Together

At St. Joseph's Catholic Primary School, we believe that every child is a unique creation of God.
We promote respect and care for one another following in the footsteps of the family Jesus wants us to be.
Caring for one another is at the centre of our school life.
We promise to provide educational opportunities and experiences to enrich the learning and well-being of the children by following the teaching of Jesus Christ.
Our school values its partnership with the Parish community and MAT, together enabling our children to become rounded, confident individuals, with an understanding of Gospel values as preparation for the world of work and life.

ONLINE SAFETY Policy

Written by:	Date reviewed:	Approved by:	Date for next review:
E Critchley	September 2024	Fr. John-Paul Evans	September 2025

Introduction

This policy sets out St Joseph's School's aims and strategies for the successful delivery of online safety. This policy should be read in conjunction with other relevant school policies such as the Safeguarding, Equal Opportunities, Curriculum, Finance, Teaching & Learning, SEND and Assessment policies. The Computing Leader in consultation with the SENCO, Leadership Team, and teachers have developed the policy. This policy is based on government recommended/statutory programmes of study. Due to the fast pace of technology innovation and constantly emerging trends, it is recommended that this policy is reviewed, at minimum, at the start of every academic cycle.

Aims

This Online Safety Policy outlines the commitment of St Joseph's to safeguard members of our school community online in accordance with statutory guidance and best practice. The policy applies to all members of the school community (including staff, learners, governors, volunteers, parents and carers, visitors) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed). St Joseph's will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using:

- logs of reported incidents
- Filtering and monitoring logs
- internal monitoring data for network activity

Roles and Responsibilities

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent.

Head Teacher

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding.
- The headteacher and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The headteacher/senior leaders are responsible for ensuring that the Designated Safeguarding Lead, IT provider/technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The headteacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.

- The headteacher/senior leaders will receive regular monitoring reports from the Designated Safeguarding Lead.
- The headteacher/senior leaders will work with the responsible Governor, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring.

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.

This review will be carried out by Father John-Paul Evans who will receive regular information about online safety incidents and monitoring reports. A member of the governing body will take on the role of Online Safety Governor to include:

- regular meetings with the Designated Safeguarding Lead
- regularly receiving (collated and anonymised) reports of online safety incidents
- checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training) is taking place as intended.
- Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually. (The review will be conducted by members of the SLT, the DSL, and the IT service provider and involve the responsible governor) - in-line with the DfE Filtering and Monitoring Standards
- reporting to relevant governors group/meeting

The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

Designated Safety Lead (DSL)

In accordance to Keeping Children Safe in Education
The DSL will:

- hold the lead responsibility for online safety, within their safeguarding role.
- Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online
- be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)

Curriculum Leads

Curriculum Leads will work with the DSL to develop a planned and coordinated online safety education programme.
This will be provided through:

- a discrete programme – ProjectEvolve and PurpleMash
- PSHE programme- You Me PSHE

- assemblies and pastoral programmes
- through relevant national initiatives and opportunities e.g. Safer Internet Day

Teaching and support staff
School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood, and signed the staff acceptable use agreement (AUA)
- they immediately report any suspected misuse or problem to Rachael Griffiths for investigation/action, in line with the school safeguarding procedures
- all digital communications with learners and parents/carers are on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- in lessons where internet use is pre-planned learners are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- where lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies
- there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

IT Provider
In accordance to the DfE Filtering and Monitoring Standards:

The IT Provider is responsible for ensuring that:

- they are aware of and follow the school Online Safety Policy and Technical Security Policy to carry out their work effectively in line with school policy
- the school technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from local authority / MAT or other relevant body
- there is clear, safe, and managed control of user access to networks and devices

- they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to Rachael Griffiths for investigation and action
- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person
- monitoring systems are implemented and regularly updated as agreed in school policies

Learners

- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should know what to do if they or someone they know feels vulnerable when using online technology.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents and carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

The school will take every opportunity to help parents and carers understand these issues through:

- publishing the school Online Safety Policy on the school website
- publish information about appropriate use of social media
- parents'/carers', newsletters, website, social media

Parents and carers will be encouraged to support the school in:

- reinforcing the online safety messages provided to learners in school.
- the safe and responsible use of their children's personal devices in the school (where this is allowed)

Teaching and Learning

Online safety has a high profile at St Joseph's School for all stakeholders. Project Evolve also provides us with the platform to provide all years with the most up to date and effective online safety lessons, to ensure we are meeting the framework "Education for Connected World". Additionally, the children will be partaking in online safety lessons during their PSHE sessions- following the scheme of "You, Me, PSHE".
We ensure this profile is maintained and that pupil needs are met by the following:

- A relevant up-to-date online safety curriculum, which is progressive from Early Years to the end of Year 6.

- Through our home/school links and communication channels, parents are kept up to date with relevant online safety matters, policies, and agreements. They know whom to contact at school if they have concerns.
- Data policies, which stipulate how we keep confidential information, are secure.
- A curriculum that is threaded throughout other curriculums and embedded in the day-to-day lives of our pupils.
- Pupils, staff, and parents have "Acceptable Use Policies" which are signed and copies freely available.
- Training for staff and governors, which is relevant to their needs and ultimately positively affects the pupils.
- Scheduled pupil voice sessions and learning walks steer changes and inform training needs.

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk known as the 4Cs:

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

Strong links between teaching online safety and the curriculum (see also Roles above) are the clearest in:

- Personal, Social and Health Education (PSHE)
- Relationships education, relationships, and sex education (HRSE)
- Computing

It is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting subject lead staff and making the most of unexpected learning opportunities as they arise.

Whenever overseeing the use of technology (devices, the Internet, new technology such as augmented reality, etc) in school or setting as homework tasks, all staff will encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites.

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age-appropriate materials and signposting, and legal issues such as copyright, plagiarism, and data law.

We recognise that online safety and broader digital resilience must be included throughout the curriculum.

Annual reviews of curriculum plans / schemes of work (including for SEND pupils) are used as an opportunity to assess the key areas of Self-image and Identity, Online relationships, Online reputation, Online bullying, Managing online information, Health, Wellbeing and lifestyle, Privacy and security, and Copyright and ownership.

How internet use enhances learning
This school:

- has a clear, progressive online safety education programme as part of the Computing/PSHE curriculum. This covers the teaching of a range of skills and behaviours which are appropriate to the age and experience of the pupils concerned and include those to:
  - STOP and THINK before they CLICK;
  - develop a range of strategies to evaluate and verify information before accepting its accuracy;
  - be aware that the author of a website/page may have a particular bias or purpose and to develop skills to recognise what that may be;
  - know how to narrow down or refine a search;
  - [for older pupils] understand how search engines work and to understand that this affects the results they see at the top of the listings;
  - understand acceptable behaviour when using an online environment/email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
  - understand how photographs can be manipulated and how web content can attract unwanted or inappropriate attention;
  - understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs, and videos and to know how to ensure they have turned-on privacy settings;
  - understand why they must not post pictures or videos of others without their permission;
  - know not to download any files – such as music files – without permission;
  - have strategies for dealing with receipt of inappropriate materials;
  - [for older pupils] understand why and how some people will 'groom' young people for sexual or extremist ideology reasons;
  - understand the impact of cyberbullying, sharing inappropriate images and trolling and know how to seek help if they are affected by any form of online bullying;
  - know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent, teacher or trusted staff member, or an organisation such as ChildLine
- plans internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- will remind pupils about their responsibilities through an end-user Acceptable Use Agreement which will be displayed throughout the school or when they log on to the school's network;
- ensures staff model safe and responsible behaviour in their own use of technology during lessons;
- ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and know that they must respect and acknowledge copyright/intellectual property rights;

- ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include risks in pop-ups; buying online; online gaming/gambling etc.

Pupils with additional needs

We use a wide range of strategies to support children with additional needs who might need extra support to keep themselves safe, especially online.

- Sensitively check pupil's understanding and knowledge of general personal safety issues using reminders and explicit prompts to link their existing knowledge of "how to keep safe" to the rules that will apply specifically to, for instance, internet use.
- Apply rules consistently to embed understanding.
- Project Evolve resources are used to help pupils transfer rules to other lessons and environments.
- Communicate rules clearly to parents and seek their support in implementing school rules at home. Working with parents and sharing information with them is relevant to all children, but this group especially.
- Careful explanations about why rules might change in different situations i.e. why it is ok to give your name and address to an adult if you are lost in town, but not when using the Internet.
- Consistent use of cause and effect linking the rules to consequences teaching realistic and practical examples of what might happen if… without frightening pupils.

Handling online safety concerns and incidents

Our staff recognise that online safety is only one element of the wider safeguarding agenda as well as being a curriculum strand of Computing and PSHE/RSHE

General concerns will be handled in the same way as any other child protection concern. Early reporting to the DSL is vital to ensure that the information contributes to the overall picture or highlights what might not yet be a problem.

Support staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets, and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence).

Procedures for dealing with online safety, concerns and incidents are detailed in the following Policies:

- Behaviour Policy and procedures (includes anti-bullying procedures)
- Acceptable Use Agreements
- Data Protection Policy, agreements, and other documentation (e.g. privacy statement, consent forms for data sharing image use etc.)

We are committed to taking all reasonable precautions to ensure online safety but recognise that incidents will occur both inside and outside school. All members of the school community are encouraged to report issues swiftly to school staff so that they can be dealt with quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the DSL/OSL on the same day wherever possible or, if out of school, the following school day.

Any concern/allegation about misuse by staff or other adult in school will always be referred directly to the Head teacher unless the concern is about the Head teacher, in

which case, the complaint will be directed to the Chair of Governors. Staff may also use the NSPCC Whistleblowing Helpline. Call 0800 028 0285 or email: help@nspcc.org.uk.

The school will actively seek support from other agencies as needed (i.e. Local Authority Safeguarding Hub, UK Safer Internet Centre's Professionals' Online Safety Helpline (03443814772), NCA CEOP. We will inform parents of online safety incidents involving their child and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or is considered illegal.

See Sections below for procedures for dealing with the sharing of nude and/or semi-nude images and/or videos, upskirting and online (cyber) bullying.

- In this school there is strict monitoring and application of the Online Safety Policy and a differentiated and appropriate range of sanctions.
- All members of the school community will be informed about the procedure for reporting online safety concerns (such as breaches of filtering, cyberbullying, illegal content etc.).
- The Designated Safeguarding Lead will be informed of any online safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The school will manage Online Safety incidents in accordance with the school Behaviour Policy where appropriate.
- The school will inform parents of any incidents or concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Safeguarding Hub and escalate the concern to the Police.
- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Safeguarding Hub

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence, and protect those carrying out the investigation. More than one member of staff should be involved in the investigation which should be carried out on a "clean" designated computer.

Incidents will be dealt with as soon as possible in a proportionate manner through normal behaviour/disciplinary procedures. It is important that, where necessary, members of the school community are made aware that incidents have been dealt with.

- Sharing nude and/or semi-nude images and/or videos
  Where incidents of the sharing of nude and/or semi-nude images and/or videos via the internet or mobile phone by those under the age of 18 are discovered , we will refer to the UK Council for (UKCIS) guidance 'Sharing nude and semi-nude images'. A copy of this document is available from the school office. Where one of the parties is over the age of 18 and the other is under 18, we will refer to it as child sexual abuse.

  All staff and other relevant adults have been issued with a copy of the UKCIS overview document (Sharing nudes and semi-nudes: how to respond to an incident) in recognition of the fact that it is generally someone other than the DSL who will first become aware of an incident. Staff, other than the DSL, must not intentionally view, copy, print, share, store or save or delete the image or ask anyone else to do so but must report the incident to the DSL as soon as possible.

It is the responsibility of the DSL to follow the guidance issued by UKCIS, decide on the next steps and whether to involve other agencies as appropriate.

It is important to understand that whilst the sharing of nude and/or semi-nude images and/or videos is illegal, pupils should be encouraged to discuss with staff situations if they have made a mistake or had a problem with this issue.

The UKCIS advice outlines how to respond to an incident of nudes and semi-nudes being shared including:

- risk assessing situations;
- safeguarding and supporting children and young people;
- handling devices and images;
- recording incidents, including the role of other agencies.
- informing parents and carers

The types of incidents which this advice covers are:

- a person under the age of 18 creates and shares nudes and semi-nudes of themselves with a peer under the age of 18;
- a person under the age of 18 shares nudes and semi-nudes created by another person under the age of 18 with a peer under the age of 18;
- a person under the age of 18 is in possession of nudes and semi-nudes created by another person under the age of 18.

- Upskirting
  All staff are aware that 'upskirting' (taking a photo of someone under their clothing) is now a criminal offence, but that pupils should be encouraged to discuss with staff situations if they have made a mistake or had a problem with this issue. If staff or other adults become aware of an incident of 'upskirting', the issue must be reported to the DSL as soon as possible.

- Cyberbullying
  Cyberbullying (also known as online bullying) can be defined as the use of information and communications technology particularly mobile devices and the internet, deliberately to upset someone else and reported incidents will be treated in the same way as any other form of bullying. The Behaviour Policy and procedures will be followed in relation to sanctions taken against the perpetrator. It is important not to treat online bullying separately to offline bullying and to recognise that some bullying will have both online and offline elements. Support will be provided to both the victim and the perpetrator. In some cases, it may be necessary to inform or involve the Police.

Many young people and adults find that using the Internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. When children are the target of bullying via mobile phones, gaming, or the Internet, they can often feel very alone, particularly if the adults around them do not understand cyberbullying and its effects. A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety. It is essential that young people, school staff and parents understand how cyberbullying is

different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

There are several statutory obligations on schools in relation to behaviour which establish clear responsibilities to respond to bullying. In particular, section 89 of the Education and Inspections Act 2006:

- every school must have measures to encourage good behaviour and prevent all forms of bullying amongst pupils. These measures should be part of the school's Behaviour Policy which must be communicated to all pupils, school staff and parents;
- gives Head teachers the ability to ensure that pupils behave when they are not on school premises or under the lawful control of school staff.

Where bullying outside school (such as online or via text) is reported to the school, it will be investigated and acted on in line with the school Behaviour Policy and procedures.

Although bullying in itself is not a specific criminal offence in the UK, it is important to bear in mind that some types of harassing or threatening behaviour or communications could be a criminal offence, for example under the Protection from Harassment Act 1997, the Malicious Communications Act 1988, the Communications Act 2003, and the Public Order Act 1986. If school staff feels that an offence may have been committed, they should seek assistance from the Police.

DfE and Childnet have produced resources and guidance that we expect staff to use to give practical advice and guidance on cyberbullying:

- Cyberbullying (along with all other forms of bullying) of any member of the school community will never be tolerated.
- There are clear procedures in place to support anyone in the school community affected by cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of cyberbullying.
- Pupils, staff, and parents will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the perpetrator, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the Police, if necessary.
- Pupils, staff, and parents will be required to work with the school to support the approach to cyberbullying and the school's online safety ethos.
- Sanctions for those involved in cyberbullying may include:
    - The perpetrator will be asked to remove any material deemed to be inappropriate or offensive.
    - A service provider may be contacted to remove content if the perpetrator refuses or is unable to delete content.
    - Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance with the Behaviour Policy and procedures and Acceptable Use Agreement.
    - Parents of both the perpetrator(s) and the victim(s) will be informed.
        - The Police will be contacted if a criminal offence is suspected.

- Harmful online challenges or hoaxes

  An online challenge will generally involve users recording themselves taking a challenge and then distributing the resulting video through social media sites, often inspiring or daring others to repeat the challenge. Whilst many will be safe and fun, others can be potentially harmful and even life threatening.

  If staff are confident children and young people are aware of, and engaged in, a real challenge that may be putting them at risk of harm, then it would be appropriate for this to be directly addressed by either the DSL or a senior leader in school. Careful consideration will be given on how best to do this, and it may be appropriate to offer focussed support to a particular age group or individual children at risk. We will take account of the fact that even with real challenges, many children and young people may not have seen it and may not be aware of it and will carefully weigh up the benefits of institution-wide highlighting of the potential harms related to a challenge against needlessly increasing children and young people's exposure to it.

  Where staff become aware of a potentially harmful online hoax or challenge, they will immediately inform the DSL who will take the appropriate action either with the pupil concerned or with the wider group where the incident involves more than one pupil.

  Where the DSL considers it necessary to directly address an issue, this can be achieved without exposing children and young people to scary or distressing content. In the response, we will consider the following questions:

  - is it factual?
  - is it proportional to the actual (or perceived) risk?
  - is it helpful?
  - is it age and stage of development appropriate?
  - is it supportive?

  A hoax is a deliberate lie designed to seem truthful. The internet and social media provide a perfect platform for hoaxes, especially hoaxes about challenges or trends that are said to be harmful to children and young people to be spread quickly.

  We will carefully consider if a challenge or scare story is a hoax. Generally speaking, naming an online hoax, and providing direct warnings is not helpful. Concerns are often fuelled by unhelpful publicity, usually generated on social media, and may not be based on confirmed or factual occurrences or any real risk to children and young people. There have been examples of hoaxes where much of the content was created by those responding to the story being reported, needlessly increasing children and young people's exposure to distressing content.

  Evidence from Childline shows that, following viral online hoaxes, children and young people often seek support after witnessing harmful and distressing content that has been highlighted, or directly shown to them (often with the best of intentions), by parents, carers, schools, and other bodies. In this respect, staff will be mindful of the advice provided by the UK Safer Internet Centre which provides guidance on dealing with online hoaxes or challenges.

  In any response, reference will be made to the DfE guidance 'Harmful online challenges and online hoaxes'.

- Sexual violence and harassment
  DfE guidance on sexual violence and harassment is referenced in Part five of 'Keeping Children Safe in Education'. All staff are aware of this guidance.

  We have a zero tolerance approach to all forms of sexual violence and harassment and will act appropriately on information which suggests inappropriate behaviour

regardless of the considered seriousness. Any incident of sexual harassment or violence (online or offline) must be reported to the DSL at the earliest opportunity. The DSL will follow the guidance as outlined in the Child Protection Policy and procedures. Sanctions will be applied in line with our Behaviour Policy and procedures.

- Misuse of school technology (devices, systems, networks, or platforms)
  Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

  These rules are defined in the relevant Acceptable Use Agreements as provided to pupils, staff, and Governors.

  Where pupils contravene these rules, the Behaviour Policy and procedures will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct and, where necessary, the school disciplinary procedures.

  The school reserves the right to withdraw, temporarily or permanently, any or all access to such technology or the right to bring mobile technology devices onto school property.

- Social media incidents
  See Social Media Policy. Social media incidents are governed by Acceptable Use Agreements. Breaches will be dealt with in line with these procedures, the Behaviour Policy and procedures (for pupils) and the staff Code of Conduct/Disciplinary procedures (for staff and other adults).

  Where an incident relates to an inappropriate, upsetting, violent or abusive social media post by an identifiable member of the school community, we will request that the post be deleted and will expect this to the actioned promptly.

  Where an offending post has been made by a third party or is anonymous, the school may report it to the hosting platform, the Police or may contact the Professionals' Online Safety Helpline (UK Safer Internet Centre) for support or assistance in accelerating the process of removal.

Data protection and data security

All pupils, staff, Governors, parents, and other adults working in or visiting school are bound by the school's Data Protection Policy and procedures a copy of which is available from the school office.

There are references to the relationship between data protection and safeguarding in key DfE documents i.e. Keeping Children Safe in Education and Data protection: a toolkit for schools which the DPO and DSL will seek to apply.

The Head teacher, DPO and Governors work together to ensure a DPA compliant framework for storing data, but which ensures that child protection is always the primary consideration and data protection processes support careful and legal sharing of information. The Data Protection Act 2018 does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Information which is sensitive and personal will be treated as 'special category personal data' for the purposes of compliance with the DPA. Legal and secure information sharing between schools, Children's Social Care and other local agencies is essential for keeping children safe and ensuring they get the support they need. Information can be shared without consent if to

gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children. As with all data sharing, appropriate organisational and technical safeguards will be in place.

All pupils, staff, Governors, volunteers, contractors, and parents are bound by the school's Data Protection Policy and procedures.

- Maintaining Information Systems Security
  Local Area Network (LAN) security issues include:
  - Users must act reasonably e.g. the downloading of large files or viewing sporting events during the working day will affect the service that others receive.
  - Users must take responsibility for their network use. For staff, flouting the school Acceptable Use Agreement may be regarded as a reason for dismissal.
  - Workstations should be secured against user mistakes and deliberate actions.
  - Servers will be located securely and physical access restricted.
  - The server operating system is secured and kept up to date.
  - Virus protection for the whole network is installed and current.
  - Access by wireless devices will be proactively managed and secured with a minimum of WPA2 encryption.

  Wide Area Network (WAN) security issues include:
  - Broadband firewalls and local CPEs (Customer Premises Equipment) are configured to prevent unauthorised access between schools.
  - Decisions on WAN security are made in partnership between school and our network provider.

The following statements apply in our school:

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet or taken off site will be encrypted.
- Portable media may not be used without specific permission followed by an anti-virus/malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The ICT coordinator/network manager will review system capacity regularly.
- Use of user logins and passwords to access the school network will be enforced – see Section 6.2 below.

The school broadband and online suppliers are Sensible IT

The Head teacher, Data Protection Officer and Governors work together to ensure a DPA compliant framework for storing data, but which ensures that child protection is always put first, and data protection processes support careful and legal sharing of information.

Password Security

We will ensure that the school network is as safe and secure as is reasonably possible and that users can only access data to which they have right of access; no user is able to access another's files without permission (or as allowed for monitoring purposes within the school's procedures); access to personal data is securely controlled in line with the school's personal data procedures; logs are maintained of access by users and of their actions while users of the system.

All users (adults and young people) will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

Passwords for new users, and replacement passwords for existing users can be allocated by Sensible IT. Any changes carried out must be notified to the member of staff responsible for issuing and coordinating password security (above).

Users will change their passwords every 6 months.

Training/Awareness:

It is essential that users are made aware of the need to keep passwords secure, and the risks attached to unauthorised access/data loss. This will apply to even the youngest of users, even if class log-ons are being used.

Members of staff will be made aware of the school's password security procedures:

- at induction;
- through the school's Online Safety Policy and procedures;
- through the Acceptable Use Agreement.

Pupils will be made aware of the school's password security procedures:

- in Computing/ICT and/or Online Safety lessons;
- through the Acceptable Use Agreement.

Audit/Monitoring/Reporting/Review:

The responsible person (Office Staff) will ensure that full records are kept of:

- User Ids and requests for password changes;
- User log-ons;
- Security incidents related to this Policy and procedures.

In the event of a serious security incident, the Police may request and will be allowed access to passwords used for encryption. Local Authority Auditors also have the right of access to passwords for audit investigation purposes.

User lists, IDs and other security related information must be given the highest security classification and stored in a secure manner. These records will be reviewed by Online Safety Coordinator at regular intervals.

<u>Use of digital and video images</u>

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, pupils and parents need to be aware of the risks associated with sharing images and with posting digital images on the Internet. Those images may remain available on the Internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement procedures to reduce the likelihood of the potential for harm:

- We gain parental permission for the use of digital photographs or video involving their child as part of the school agreement form when their child joins the school. This is a once in a school lifetime consent. Parents are required to inform the school if their consent changes.
- We seek consent for the publication of images from pupils.

- When we publish images or video, we will inform pupils and parents before publishing, so they have a chance to object as is their legal right under DPA 2018.
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced digital materials. Photo file names/tags do not include full names to avoid accidentally sharing them.
- When using digital images, staff will inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Staff are governed by their contract of employment, the staff Code of Conduct and sign the school's Acceptable Use Agreement. This includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils.
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose.
- Staff are permitted to take digital/video images to support educational aims, but must follow school procedures concerning the sharing, distribution, and publication of those images. Those images will, wherever possible only be taken on school equipment. Members of staff may occasionally use personal phones to capture photos or videos of pupils. These will be appropriate, linked to school activities, taken without secrecy, and not captured in a one-to-one situation. Photos will always be moved to school storage as soon as possible after which they are deleted from personal devices and/or cloud services (Note: many phones automatically back up photos).
- Staff will ensure that when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Digital images/videos are stored on the school network in line with the retention schedule of the school Data Protection Policy.
- Pupils are taught about how images can be manipulated in their online safety education programme and are taught to consider how to publish for a wide range of audiences which might include Governors, parents, or younger children as part of their ICT scheme of work;
- Pupils are taught that they should not post images or videos of others without their consent. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they or a friend are subject to bullying or abuse.
- Staff and parents are regularly reminded about the importance of not sharing without consent, due to child protection concerns (e.g. children looked-after often have restrictions for their own protection) data protection, religious or cultural reasons or simply for reasons of personal privacy.
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high-profile publications the school will obtain individual parental or pupil consent for its long-term use. A model Consent Form can be found in Kym Allan Health and Safety Consultants Ltd. (KAHSC) General Safety Series G21.
- A pupil's work can only be published with the consent of the pupil and parents. We will seek the consent of the pupil first and then, if necessary, the parents.

Filtering & Monitoring

In accordance to the DfE guidance (for England) on filtering and monitoring in "Keeping Children Safe in Education":

The school filtering and monitoring provision is agreed by senior leaders, governors and the IT Service Provider and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours.

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and the IT service provider will have technical responsibility.
The filtering and monitoring provision is reviewed (at least annually) by senior leaders, the Designated Safeguarding Lead and a governor with the involvement of the IT Service Provider.

Filtering

- the school manages access to content across its systems for all users and on all devices using the schools internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre Appropriate filtering.
- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- there are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective
- there is a clear process in place to deal with, and log, requests/approvals for filtering changes.
- filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.
- the school has (if possible) provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/learners, etc.)
- the school has a mobile phone policy and where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice.
- access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.

If necessary, the school will seek advice from, and report issues to, the SWGfL Report Harmful Content site.

Monitoring
The school has monitoring systems in place to protect the school, systems and users:

- The school monitors all network use across all its devices and services.
- monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that the network (and devices) are monitored.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.

The school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through the use of the appropriate blend of strategies informed by the school's risk assessment. These may include:

- physical monitoring (adult supervision in the classroom)
- internet use is logged, regularly monitored and reviewed
- filtering logs are regularly analysed and breaches are reported to senior leaders
- pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.
- where possible, school technical staff regularly monitor and record the activity of users on the school technical systems
- use of a third-party assisted monitoring service to review monitoring logs and report issues to school monitoring lead(s)