

St Joseph's Catholic Primary School

Online Safety Policy

May 2023



We are children of God; we achieve, believe and care.

## **Scope of the Online Safety Policy**

This Online Safety Policy outlines the commitment of St Joseph's Catholic Primary School to safeguard members of our school community online in accordance with statutory guidance and best practice.

This Online Safety Policy applies to all members of the school community (including staff, pupils, volunteers, parents and carers, visitors, community users) 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 Catholic Primary School 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.

## **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. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

### *Headteacher and senior leaders*

- 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, though the day-to-day responsibility for online safety may be delegated to the Online Safety Lead.
- 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 Online Safety Lead, 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 Online Safety Lead.

### *Governors*

The DfE guidance "Keeping Children Safe in Education" states: "Governing bodies and proprietors should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children's welfare ... this includes ... online safety"

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy e.g. by asking the questions posed in the UKCIS document “Online Safety in Schools and Colleges – questions from the Governing Body”.

This review will be carried out by the safeguarding link governor(s) who will receive regular information about online safety incidents and monitoring reports, including:

- Meetings with the Online Safety Lead
- 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)
- Reporting to relevant governors group/meeting
- Membership of the school Online Safety Group
- Occasional review of the filtering change control logs and the monitoring of filtering logs (where possible)

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

#### *Online Safety Lead*

The Online Safety Lead will:

- Work closely with the Designated Safeguarding Lead (DSL), where these roles are not combined.
- Take day-to-day responsibility for online safety issues, being aware of the potential for serious child protection concerns.
- Have a leading role in establishing and reviewing the school online safety policies/documents.
- Promote an awareness of and commitment to online safety education / awareness raising across the school and beyond.
- Liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated.
- Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents.
- Receive reports of online safety incidents and create a log of incidents to inform future online safety developments.
- Provide (or identify sources of) training and advice for staff, governors, parents, carers and pupils.
- Liaise with BWCET technical staff, pastoral staff and support staff (as relevant).
- Meet with the safeguarding link governor(s) to discuss current issues, review (anonymised) incidents and if possible, filtering and monitoring logs.
- Attend relevant governing body meetings/groups.
- Report regularly to headteacher/senior leadership team.

#### *Designated Safeguarding Leads (DSLs)*

The Designated Safeguarding Lead should be trained in online safety issues and be aware of the potential for serious safeguarding issues to arise from:

- Sharing of personal data

- Access to illegal/inappropriate materials
- Inappropriate online contact with adults/strangers
- Potential or actual incidents of grooming
- Online bullying.

#### *Curriculum Leads*

Curriculum Leads will work with the Online Safety Lead to develop a planned and coordinated online safety education programme e.g. ProjectEVOLVE .

This will be provided through:

- Our Computing curriculum
- Our PHSE and RSE curriculum
- Assemblies and pastoral programmes
- Through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

#### *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 a DSL or member of the SLT for investigation/action, in line with the school safeguarding procedures.
- All digital communications with pupils and parents/carers should be 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 pupils 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 pupils should be 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.
- Younger children use the child friendly search engine Swiggle for internet searches. As the children progress through Key Stage 2, they will receive online safety education on safe use of search engines such as Google and will begin to use Google for internet searches. Google 'safe search' is enforced on all devices.
- They have 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.

#### *Pupils*

- Are responsible for using the school digital technology systems in accordance with the pupil acceptable use agreement and Online Safety Policy.
- 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.
  - Providing them with a copy of the pupils' acceptable use agreement.
  - Publish information about appropriate use of social media relating to posts concerning the school.
  - Seeking their permissions concerning digital images, cloud services etc (see parent/carer AUA in the appendix).
  - Parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

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

- Reinforcing the online safety messages provided to pupils in school.

#### **Professional Standards**

There is an expectation that required professional standards will be applied to online safety as in other aspects of school life i.e., policies and protocols are in place for the use of online communication technology between the staff and other members of the school and wider community, using officially sanctioned school mechanisms.

#### **Acceptable Use**

The school has defined what it regards as acceptable/unacceptable use and this is outlined in our acceptable use agreements (AUAs). The Online Safety Policy and acceptable use agreements define acceptable use at the school. The acceptable use agreements will be communicated/re-enforced through:

- Staff induction and handbook
- Communication with parents/carers
- Built into Computing lessons
- School website

When using communication technologies, the school considers the following as good practice:

- When communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school: WeDuc, ClassDojo, school email.

- Any digital communication between staff and pupils or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content. Personal e-mail addresses, text messaging or social media must not be used for these communications.
- Staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community
- Users should immediately report to a nominated person – in accordance with the school policy – the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication
- Relevant policies and permissions should be followed when posting information online e.g., school website and social media. Only school e-mail addresses should be used to identify members of staff and pupils.

### **Reporting and responding**

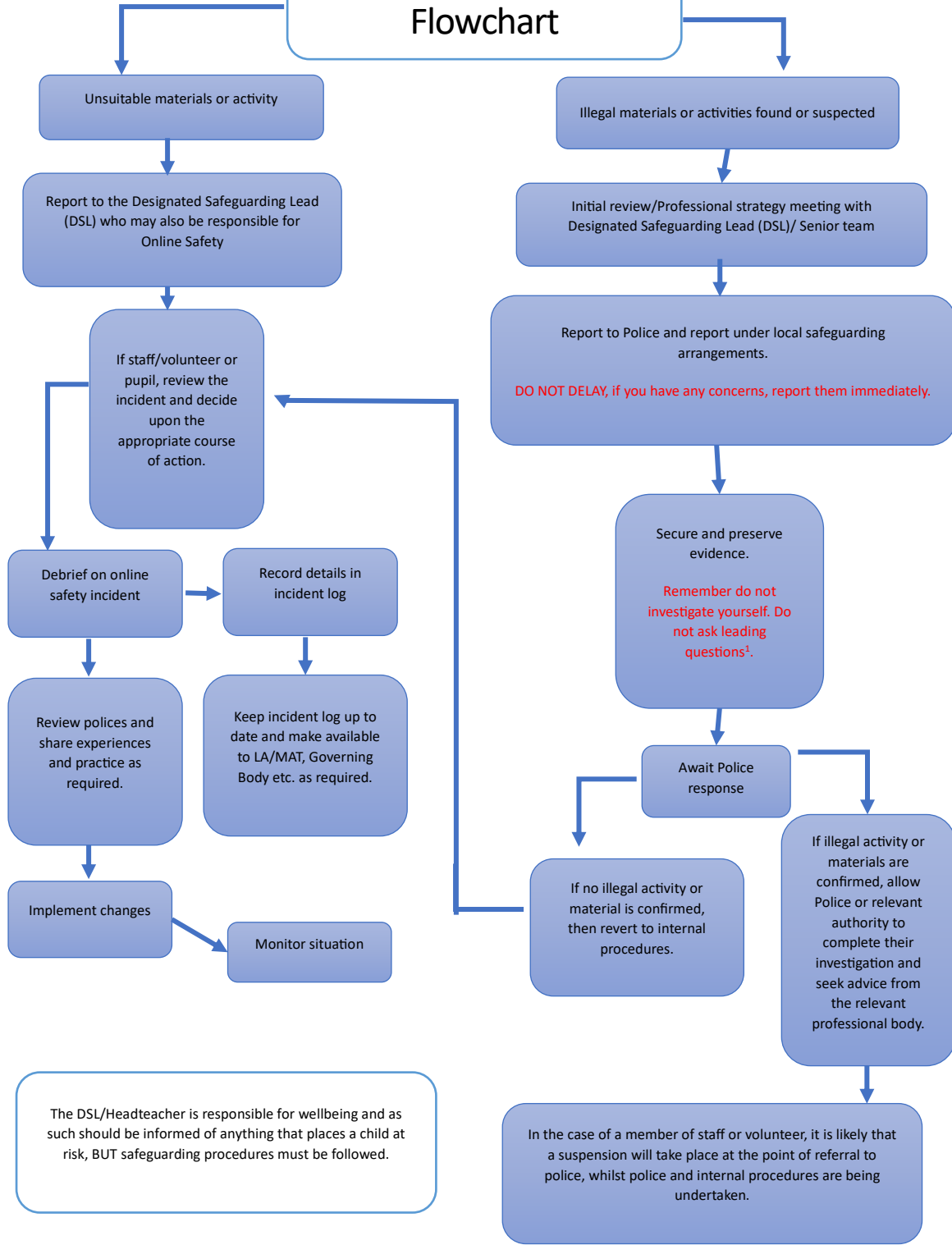
The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- There are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- All members of the school community will be made aware of the need to report online safety issues/incidents.
- Reports will be dealt with as soon as is practically possible once they are received.
- The Designated Safeguarding Lead, Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.
- If there is any suspicion that the incident involves any illegal activity or the potential for serious harm, the incident must be escalated through the agreed school safeguarding procedures.
- Any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors
- Where there is no suspected illegal activity, devices may be checked using the following procedures:
  - one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
  - conduct the procedure using a designated device that will not be used by pupils and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
  - ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
  - record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form.

- once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
  - internal response or discipline procedures
  - involvement by local authority / MAT (as relevant)
  - police involvement and/or action
- It is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively.
- There are support strategies in place e.g., peer support for those reporting or affected by an online safety incident.
- Incidents should be logged on CPOMS.
- Relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. BWCET, police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
- Those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant).
- Learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
  - staff, through regular briefings
  - pupils, through assemblies/lessons
  - parents/carers, through newsletters, school social media, website
  - governors, through regular safeguarding updates

The school will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.

# Online Safety Incident Flowchart



The DSL/Headteacher is responsible for wellbeing and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.

In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.



## **School actions**

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures.

## **Online Safety Education Programme**

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum for all year groups matched against a nationally agreed framework. We follow the Teach Computing curriculum for Computing and the Life to the Full curriculum for RSE/PSHE.
- Lessons are matched to need, are age-related and build on prior learning.
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes.
- Pupil need and progress are addressed through effective planning and assessment.
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; RSE; Literacy etc.
- It incorporates and makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.
- The programme will be accessible to pupils at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- The online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.

## **Staff and Volunteers**

All staff will receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- Online safety training will be an integral part of the school's annual safeguarding and data protection training for all staff
- All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours.

## **Governors**

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in technology, online safety, health and safety or safeguarding. This may be offered in several ways such as:

- Attendance at training provided by BWCET or other relevant organisation (e.g., SWGfL)
- Participation in school training / information sessions for staff or parents.

## **Families**

The school will seek to provide information and awareness to parents and carers through:

- Regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes
- Opportunities for engagement with parents/carers on online safety issues through awareness workshops, parent/carer evenings etc
- The pupils – who are encouraged to pass on to parents the online safety messages they have learned in lessons.
- Letters, newsletters and the school website.
- High profile events and campaigns e.g. Safer Internet Day.
- Reference to the relevant web sites/publications, e.g. SWGfL; [www.saferinternet.org.uk/](http://www.saferinternet.org.uk/); [www.childnet.com/parents-and-carers/](http://www.childnet.com/parents-and-carers/)

## **Technology**

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The school should ensure that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection.

## **Filtering**

- The school filtering policies are agreed by senior leaders and BWCET technical staff and are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents/behaviours.
- The school manages access to content across its systems for all users. The filtering provided meets the standards defined in the UK Safer Internet Centre Appropriate filtering.
- Access to online content and services is managed for all users.
- Illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC 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.
- There is a clear process in place to deal with requests for filtering changes.
- The school has provided differentiated user-level filtering (allowing different filtering levels for different groups of users: staff/pupils, etc.)
- Younger pupils will use the child friendly/age-appropriate search engines Swiggle.
- Filtering logs are regularly reviewed and alert the school to breaches of the filtering policy, which are then acted upon.

## **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.

- An appropriate monitoring strategy for all users has been agreed and users are aware that the network is monitored. There is a staff lead responsible for managing the monitoring strategy and processes.
- 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.
- Technical monitoring systems are up to date and managed and logs/alerts are regularly reviewed and acted upon.

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 strategy 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

### **Technical security**

The school technical systems will be managed in ways that ensure that the school meets recommended technical requirements.

- All users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually.
- All users (adults and pupils) have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details. Users must immediately report any suspicion or evidence that there has been a breach of security.
- All school networks and system will be protected by secure passwords. Passwords must not be shared with anyone. All users will be provided with a username and password and school will keep an up-to-date record of users and their usernames.
- Records of pupil usernames and passwords can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date endpoint (anti-virus) software.
- An agreed system is in place for the provision of temporary access of 'guests', (e.g., trainee teachers, supply teachers, visitors) onto the school systems.
- The use of removable media (e.g., memory sticks/hard drives/CDs/DVDs) should be avoided wherever possible by users on school devices.
- Systems are in place that prevent the unauthorised sharing of personal data unless safely encrypted or otherwise secured.

### **Social media**

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

- Ensuring that personal information is not published.
- Education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions.
- Risk assessment, including legal risk.
- Guidance for pupils, parents/carers.

School staff should ensure that:

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

When official school social media accounts are established, there should be:

- A process for approval by senior leaders.
- Clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff where possible.
- A code of behaviour for users of the accounts.
- Systems for reporting and dealing with abuse and misuse.
- Understanding of how incidents may be dealt with under school disciplinary procedures.

Personal use

- Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.

Monitoring of public social media

- As part of active social media engagement, the school may pro-actively monitor the Internet for public postings about the school.
- The school should effectively respond to social media comments made by others according to a defined policy or process.
- When parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.

## **Digital and video images**

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- The school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance and policies.
- When using digital images, staff will inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images.
- Staff/volunteers must be aware of those pupils whose images must not be taken/published. Those images should only be taken on school devices. The personal devices of staff should not be used for such purposes.
- Parents/carers are welcome to take videos and digital images of their children at school events for their own personal use, where we have relevant permissions in place for all children. To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images.
- Care should be taken when sharing digital/video images that pupils are appropriately dressed.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with the Online Safety Policy.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are taken for use in school or published on the school website/social media.
- Parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy.
- Images will be securely stored in line with the school retention policy.

## **Online publishing**

The school communicates with parents/carers and the wider community and promotes the school through:

- Public-facing school website
- Social media (Facebook and Twitter)
- WeDuc 'Reach More Parents' app

The school website is managed/hosted by school admin staff and senior leaders. The school ensures that online safety policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is least risk to members of the school community, through such publications.

Where pupil work, images or videos are published, their identities are protected, and full names are not published.

## **Data Protection**

The school:

- Has a Data Protection Policy.
- Implements the data protection principles and can demonstrate that it does so.
- Has paid the appropriate fee to the Information Commissioner's Office (ICO).
- Has appointed an appropriate Data Protection Officer (DPO) who has effective understanding of data protection law and is free from any conflict of interest. The school may also wish to appoint a Data Manager and Systems Controllers to support the DPO.
- Has a 'Record of Processing Activities' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it.
- The Record of Processing Activities lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis is listed.
- Has an 'information asset register' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it
- Information asset register lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis will have also been listed.
- Will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for. The school 'retention schedule' supports this.
- Data held is accurate and up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals.
- Provides staff, parents, volunteers, teenagers, and older children with information about how the school looks after their data and what their rights are in a clear Privacy Notice (see Privacy Notice section in the appendix).
- Has procedures in place to deal with the individual rights of the data subject, e.g. one of the dozen rights applicable is that of Subject Access which enables an individual to see/have a copy of the personal data held about them.
- Carries out Data Protection Impact Assessments (DPIA) where necessary e.g. to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier.
- Has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors.
- Understands how to share data lawfully and safely with other relevant data controllers.
- Has clear and understood policies and routines for the deletion and disposal of data.
- Reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.
- Has a Freedom of Information Policy which sets out how it will deal with FOI requests.

- Provides data protection training for all staff at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.

When personal data is stored on any mobile device or removable media the:

- Data will be encrypted, and password protected.
- Device will be password protected. (Be sure to select devices that can be protected in this way).
- Device will be protected by up-to-date endpoint (anti-virus) software.
- Data will be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Can recognise a possible breach, understand the need for urgency and know who to report it to within the school.
- Can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to in the school.
- Only use encrypted data storage for personal data.
- Will not transfer any school personal data to personal devices. Procedures should be in place to enable staff to work from home (i.e. VPN access to the school network, or a work laptop provided).
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption, a secure email account (where appropriate), and secure password protected devices.

## **Outcomes**

The impact of the Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, pupils; parents/carers and is reported to relevant groups:

- There is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness, and training
- There are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and Governors
- Parents/carers are informed of patterns of online safety incidents as part of the school's online safety awareness raising
- Online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate
- The evidence of impact is shared with other schools, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.