



Be the Best You Can,  
Guided by God

Our four Christian values that guide us

**LOVE**  
**HONESTY RESPECT**  
**RESILIENCE**

# **BOLNEY CEP SCHOOL**

## **Online Safety Policy**

<b>Reviewed</b>	<b>Autumn 2024</b>
<b>Next Review</b>	<b>Autumn 2026</b>

### **Our Whole Child Vision:**

**Each child is unique. We partner with families to nurture the ‘whole child’ – by understanding their specific emotional, spiritual and learning needs – so children flourish. Children leave us as fearless lifelong learners, ready to meet the world with self-confidence, curiosity and resilience.**

This vision has grown from our belief in the Bible verse:  
***“Do for other people what you want them to do for you.”***  
Luke 6:31 International Children’s Bible



Be the Best You Can,  
Guided by God

# **BOLNEY CE PRIMARY SCHOOL**

## **ONLINE SAFETY POLICY, including Social Media Policy**

*Adopted from WSCC Recommendation tool: **SWGfL 360 Groups – online safety self review tool for organisations working with children***

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

This Online Safety Policy outlines the commitment of Bolney CEP 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, 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.

Bolney CEP 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.

Our policy is available on the school website and the Acceptable Use agreements are sent home to families.

### **Schedule for development, monitoring and review**

The Online Safety Policy will be reviewed every two years or more regularly if any significant new technological developments, threats to online safety or incidents takes place.

If a serious online safety incident takes place, the DSL should inform *LADO, police/ IFD as required*

### **Policy and leadership**

#### **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 is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.
- 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 is responsible for ensuring that the Computing 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 will receive regular monitoring reports from the Computing Lead.
- The headteacher will work with SBM and JSPC 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. Governors will receive regular information about online safety incidents and monitoring reports. This will include:

- meetings with the Designated Safeguarding Lead / Computing Lead
- receiving reports of online safety incidents to the governing body safeguarding committee
- 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 annually. (The review will be conducted by members of the SLT, the SBM, and the IT service provider and involve governors) - in-line with the DfE Filtering and Monitoring Standards
- Receiving basic cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards

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)**

The DSL/ Computing Lead will:

- hold the lead responsibility for online safety, within their safeguarding role.
- Receive relevant 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
- meet regularly with governors to discuss current issues and ensuring that annual (at least) filtering and monitoring checks are carried out
- attend relevant governing body meetings
- receive reports of online safety incidents via CPOMs, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments
- decide whether online safety incidents should be referred 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)

## **Computing Lead**

The Computing Lead will also:

- 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
- provide training, information and advice for staff/governors/parents/carers/learners
- liaise with technical staff and support staff (as relevant)
- receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined In Keeping Children Safe in Education:
  - content
  - contact
  - conduct
  - commerce

## **Curriculum Leads**

Curriculum Leads will develop a planned and coordinated online safety education programme.

This will be provided through:

- a discrete computing unit of work
- Learning for Life lessons
- A mapped cross-curricular unit
- assemblies
- 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 the Headteacher 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 and have a good understanding of research skills

- they supervise and monitor the use of digital technologies 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**

The school has an IT provider: JSPC Computer Services. It is the responsibility of the school to ensure that the provider adheres to all the required online safety measures. It is also important that the provider follows and implements school Online Safety Policy and procedures.

The IT Provider is responsible for ensuring that:

- they are aware of and follow the school Online Safety 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
- 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 the Headteacher 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.*

### **Learners**

- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreements
- 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.

### **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
- parents' consultations, 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 learners 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 wider community, using officially sanctioned school mechanisms.

### **Acceptable use**

The school has defined what it regards as acceptable/unacceptable use and this is shown in Acceptable use agreements – see separate documents

An Acceptable Use Agreement outlines a school's expectations on the responsible use of technology by its users. There is an Acceptable Use agreement for staff/ volunteers/ and pupils, which is also sent to parents.

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
- communication with parents/carers
- built into education sessions with pupils/ signed agreements
- school website
- peer support

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.

- any digital communication between staff and learners or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content. *Personal e-mail addresses 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 learners.

### **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, Computing 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 (see flowchart and user actions chart in the appendix), the incident must be escalated through the agreed school safeguarding procedures, this may include
  - Non-consensual images
  - Self-generated images
  - Terrorism/extremism
  - Hate crime/ Abuse
  - Fraud and extortion
  - Harassment/stalking
  - Child Sexual Abuse Material (CSAM)
  - Child Sexual Exploitation Grooming
  - Extreme Pornography
  - Sale of illegal materials/substances
  - Cyber or hacking offences under the Computer Misuse Act
  - Copyright theft or piracy
- 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 and the local authority

- 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 learners 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
  - 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
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; 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
- learning from the incident (or pattern of incidents) will be provided to:
  - the Governing Body for regular safeguarding updates and for consideration of updates to policies or education lessons and to review how effectively the report was dealt with
  - staff, through regular briefings
  - learners, through assemblies/lessons
  - parents/carers, through newsletters, school social media, website
  - local authority/external agencies, as relevant
  - The school will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.

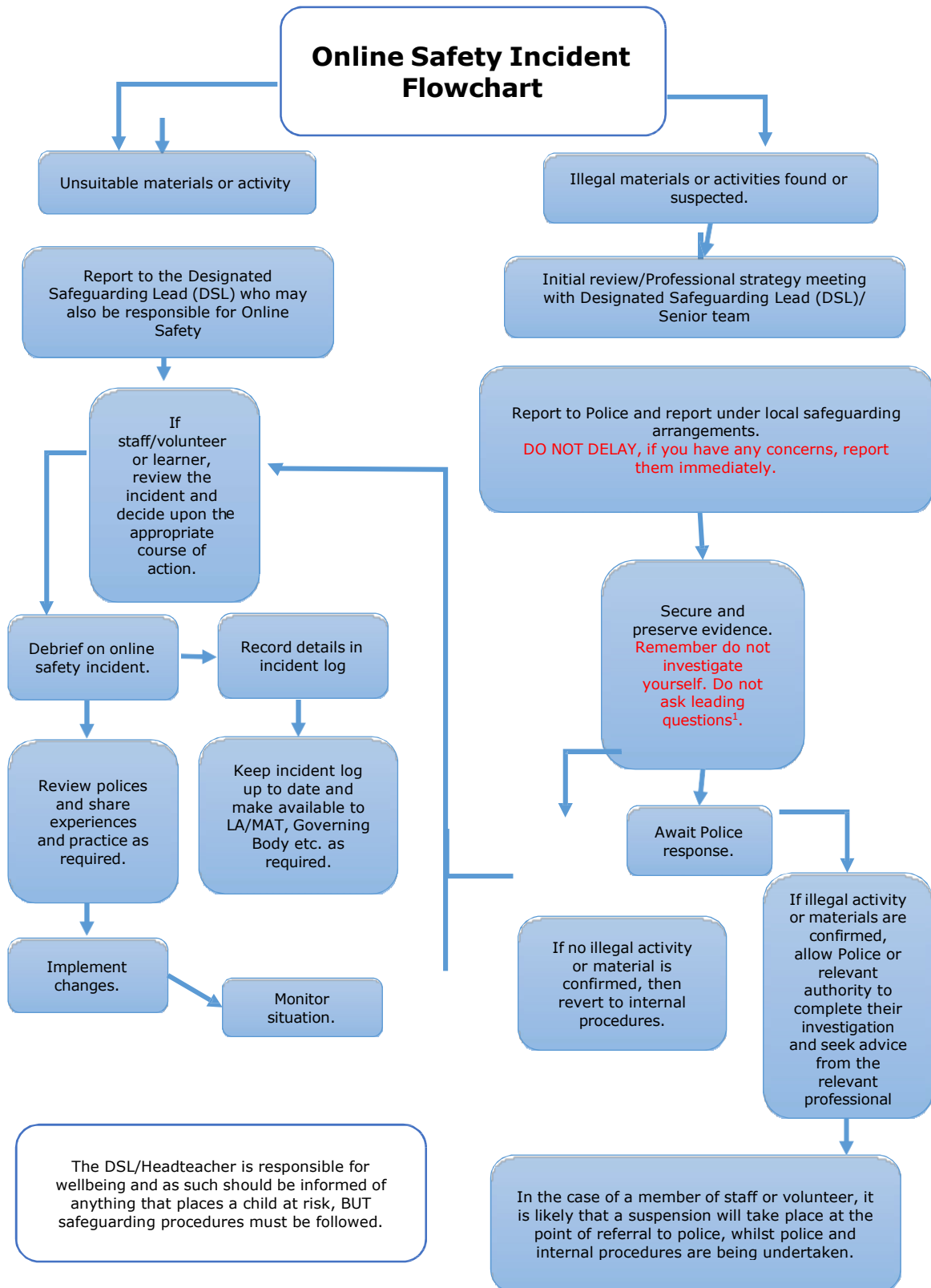
#### School actions

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.

## Online Safety Incident Flowchart



## **Online Safety Education**

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

A planned online safety curriculum for all year groups and regularly taught in a variety of contexts.

- 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
- Learner 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. Learning for Life, English
- it incorporates relevant national initiatives e.g. Safer Internet Day and Anti-bullying week
- the curriculum will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- vulnerability is actively addressed as part of a personalised online safety curriculum e.g., for victims of abuse and SEND.
- learners should be helped to understand the need for the acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school. Acceptable use is reinforced across the curriculum, with opportunities to discuss how to act within moral and legal boundaries online.
- staff should act as good role models in their use of digital technologies and the internet
- in lessons where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material in internet searches
- where learners are allowed to search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites the young people visit
- it is accepted that from time to time, for good educational reasons, students may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for a specific planned period of study.
- the online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.

## **Contribution of Learners**

The school acknowledges, learns from, and uses the skills and knowledge of learners in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for the school community and how this contributes positively to the personal development of young people. Their contribution is recognised through:

- *opportunity to canvass learner feedback and opinion.*
- *appointment of digital leaders/Learning for Life Champions*
- *learners contribute to the online safety education programme e.g. digital leaders leading lessons*

*for younger learners, online safety campaigns*

- *contributing to online safety events with the wider school community e.g. parents' evenings, family learning etc.*

### **Staff/volunteers**

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

- formal online safety and data protection training will be made available to all staff. This will be regularly updated and reinforced.
- the training will be 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. This may be offered in several ways such as:

- attendance at training provided by the local authority
- participation in school training / information sessions for staff or parents (this may include attendance at assemblies/lessons).

A higher level of training may be made available as required. This could include:

- Cyber-security training (at least at a basic level)
- Training to allow the governor to understand the school's filtering and monitoring provision, in order that they can participate in the required checks and review.

### **Families**

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

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

- regular communication, awareness-raising, online training and engagement on online safety issues, curriculum activities and reporting routes
- the learners – who are encouraged to pass on to parents the online safety messages they have learned in lessons
- letters, newsletters, website
- high profile events / campaigns e.g. Safer Internet Day
- reference to the relevant web sites/publications
- Sharing good practice with other schools in the local authority

## **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 and explain that everyone is responsible for online safety and data protection.

## **Filtering & Monitoring**

The school filtering and monitoring provision is agreed by senior leaders, governors and the IT Service Provider and is regularly reviewed 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 SBM/ IT service provider will have technical responsibility

The filtering and monitoring provision is reviewed by SBM and the DSL, with the involvement of the IT Service Provider.

- checks on the filtering and monitoring system are carried out by the IT Service Provider with the involvement of the SBM and DSL, in particular when a safeguarding risk is identified, there is a change in working practice, e.g. remote access or new technology is introduced

## **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 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.

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 DSL, 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. 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.
- SBM/ DSL regularly monitor 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)

### **Technical Security**

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

- responsibility for technical security resides with SLT who may delegate activities to identified roles.
- 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 IT service provider and will be reviewed annually by the SLT
- password policy and procedures are implemented, consistent with guidance from the National Cyber Security Centre
- all users 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.
- all school networks and system will be protected by secure passwords. Passwords must not be shared with anyone.
- the administrator passwords for school systems are kept in a secure place.
- there is a risk-based approach to the allocation of learner usernames and passwords.
- there will be regular reviews and audits of the safety and security of school technical systems
- servers, wireless systems and cabling are securely located and physical access restricted
- 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 software.
- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud,
- SBM is responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied.

- an appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person
- use of school devices out of school is regulated by an acceptable use statement that a user consents to when the device is allocated to them
- personal use of any device on the school network is regulated by acceptable use statements that a user consents to when using the network
- staff members are not permitted to install software on a school-owned devices without the consent of the SLT/IT service provider
- removable media is not permitted unless approved by the SLT/IT service provider
- systems are in place to control and protect personal data
- guest users are provided with appropriate access to school systems based on an identified risk profile.

### **Mobile technologies**

The school acceptable use agreements for staff, volunteers and learners, outline the expectations around the use of mobile technologies.

#### Personal devices:

- there is a clear policy covering the use of personal mobile devices on school premises for all users. Staff may bring mobile phones on to school site but their access is restricted to break times in areas where there are no children, for example staffroom.
- If personal mobile phones are brought to school by pupils, their use is not permitted, appropriate, safe and secure storage is made available. All mobile phones should be handed in to class teacher or office on entry to school.
- the expectations for taking/storing/using images/video aligns with the school's acceptable use policy and use of images/video policy. The non-consensual taking/using of images of others is not permitted.
- owners are liable for loss/damage or malfunction of personal devices, not the school
- there is clear advice and guidance at the point of entry for visitors to acknowledge school requirements
- education about the safe and responsible use of mobile devices is included in the school online safety education

#### Social media

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners 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 learners, parents/carers

School staff should ensure that:

- No reference should be made in social media to learners, parents/carers.
- 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
- 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. Where a personal account is used which impacts on the school it must be clear that the member of staff is not communicating on behalf of the school. 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
- the school permits reasonable and appropriate access to personal social media sites during school hours, for example during lunch periods

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.
- 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.

School use of social media for professional purposes will be checked regularly by a senior leader and the Computing Lead to ensure compliance with the social media, data protection, communications, digital image and video policies. In the event of any social media issues that the school is unable to resolve support may be sought from the Professionals Online Safety Helpline.



The social media policy provides more detailed guidance on the school's responsibilities and on good practice.

### **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 / policies.
- when using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images.
- staff/volunteers must be aware of those learners 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
- in accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites
- staff and volunteers are allowed to take digital/video images, 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 learners are appropriately dressed
- learners must not take, use, share, publish or distribute images of others without their permission
- photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with Online Safety Policy
- learners' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- permission from parents or carers will be obtained before photographs of learners are taken for use in school or published on the school website/social media.
- 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 website
- Social media
- Online newsletters

The school website is managed/hosted by eSchools. 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 learner work, images or videos are published, their identities are protected, and full names are not published.

The school public online publishing provides information about online safety e.g., publishing the schools Online Safety Policy and acceptable use agreements on the school website.

The website includes an online reporting process for parents and the wider community to register issues and concerns to complement the internal reporting process.

## **Data Protection**

Personal data will be recorded, processed, transferred, and made available according to the current data protection legislation.

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.
- 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 with information about how the school looks after their data and what their rights are in a clear Privacy Notice
- has procedures in place to deal with the individual rights of the data subject, e.g. 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.
- 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 are in place to enable staff to work from home (i.e. VPN access to the school network / a work laptop).
- 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
- 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, learners; 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.

### **Computer Misuse and Cyber Choices Policy**

All key stakeholders, including the school IT service provider, JSPC, have responsibility for the safeguarding of young people from computer misuse and are aware of the Cyber Choices programme led by the National Crime Agency (NCA) and managed locally by Regional Organised Crime Units. The risks to young people of crossing the line into committing cybercrimes is a safeguarding issue. This often happens without the individual even realising, young people need support in making the right #CyberChoices in their use of technology. Young people with an interest in technology, a high IQ, and an appetite to engage in risky behaviours are considered to be at a higher risk of committing a cyber offence, but many first-time offenders are also unaware of what the law governing cyber offences actually is. The average age of first-time cyber offenders in the UK has fallen significantly in recent years. The Cyber Choices programme works with individuals committing, or at risk of committing, cybercrimes which can only be carried out with technology, where devices are both the tool for committing the crime, and the target of the crime. All staff are made aware of the safeguarding risks of computer misuse.

All staff are familiar with the [NCA Hacking it Legal Leaflet\\*](#), which explains Cyber Choices and the Computer Misuse Act 1990, and lists recommended resources for teachers to use.

Staff are aware of the role of their local Regional Organised Crime Unit as their point of contact for Cyber Choices referrals.

Learners agree to the Acceptable Use Policy (AUP) which outlines acceptable online behaviours and explains that some online activity is illegal. Acceptable computer use is reinforced across the curriculum, with opportunities to discuss how to act within moral and legal boundaries online, with reference to the Computer Misuse Act 1990.

Any breach of the AUP or activity by a learner that may constitute a cybercrime, in school or at home, will be referred to the Designated Safeguarding Lead for consideration as a safeguarding risk.

Where the DSL believes that the learner may be at risk of committing cybercrimes, or to already be committing cybercrimes, a referral to the local [Cyber Choices](#) programme will be made (contact details for all Regional Organised Crime Units are available in the “what to do if you’re concerned” section at the bottom of the [NCA Cyber Choices page](#)). Where the DSL is unsure if a learner meets the referral criteria, advice should be sought from the local Cyber Choices team.

Parents also have the opportunity report potential cybercrime directly to the local Cyber Choices team but are recommended to make school-based concerns through the DSL.

The IT service provider is aware of the safeguarding requirement to refer concerns about computer misuse to the Designated Safeguarding Lead and has a clear process to follow in order to do so. Schools will need to contact their local [ROCU / Cyber Choices](#) team regarding local processes.

## Responding to incidents of misuse – flow cha

