



# **Online Safety Policy**

**Wellington Primary School**  
**Dudley Hill Road, Eccleshill, Bradford BD2 3DE**

This policy applies to all members of the school community (including staff, learners, 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).

Version: [1]  
Date developed: [17/07/2023]  
Next review date: [17/07/2024]

# CONTENTS

<b>THIS POLICY</b>	2
<b>Scope Of The Online Safety Policy</b>	2
<b>Policy Development, Monitoring and Review</b>	2
<b>Responsibilities</b>	Error! Bookmark not defined.
<b>Designated Safeguarding Lead (DSL) / Head Teacher</b>	3
<b>Process For Monitoring The Impact Of The Online Safety Policy</b>	5
<b>POLICY &amp; LEADERSHIP</b>	6
<b>Responsibilities</b>	6
<b>Professional Standards</b>	10
<b>ONLINE SAFETY POLICY</b>	11
<b>Acceptable Use</b>	11
<b>Reporting And Responding</b>	13
<b>Responding To Learner Actions</b>	15
<b>Responding to Staff / Volunteer / Visitor Actions</b>	15
<b>Online Safety Education Programme</b>	16
<b>Contribution of Learners</b>	17
<b>Staff / Volunteers</b>	17
<b>Governors</b>	19
<b>Families</b>	19
<b>Adults And Agencies</b>	19
<b>TECHNOLOGY</b>	20
<b>Filtering</b>	20
<b>Monitoring</b>	20
<b>Technical Security</b>	21
<b>Digital Media, The School Website &amp; Social Media</b>	22
<b>Digital and video images</b>	23
<b>Online Publishing</b>	24
<b>Data Protection</b>	24
<b>OUTCOMES</b>	26

# **THIS POLICY**

This policy and appendices have been developed using the current guidance from the South West Grid For Learning which was recommended to us by our Consultant at The Curriculum Innovation Centre Bradford, considering all current and relevant issues, in a whole school context, linking with other relevant policies such as our school's Safeguarding Policy, Behaviour Policy and Anti-Bullying Policy.

<https://swgfl.org.uk/resources/online-safety-policy-templates/>

The main policy document and appendices have been developed as follows:

- The sections match the order of the aspects in the 360° Online Safety Self Review For Schools.
- The statements take account of updated guidance e.g. Keeping Children Safe In Education, Behaviour In Schools and Searching, Screening & Confiscation.
- It reflects ongoing changes in the use of technology and its related behaviours.

## **Scope Of The Online Safety Policy**

This Online Safety Policy outlines the commitment of Wellington 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, volunteers, parents and carers, visitors and 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).

Wellington Primary School deals with all concerns about misuse within this policy and associated behaviour and anti-bullying policies. The school will inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school: via a phone call followed up by a letter (see appendix for proforma).

## **Policy Development, Monitoring and Review**

This Online Safety Policy has been developed by the Computing Curriculum Lead, the Headteacher DSL, Senior Leaders and Governors.

# School Responsibilities

<b>Designated Safeguarding Lead (DSL)</b>	<b>Head Teacher</b>	<b>Joy Wood</b>
Deputy Safeguarding Lead 1	Deputy Head	Aaron Sidebottom
Deputy Safeguarding Lead 2	Assistant Head	Catherine Berry
Senior Leaders	Deputy Head	Aaron Sidebottom
	Assistant Head	Catherine Berry
Online Safety Lead 1	Deputy Head	Aaron Sidebottom
Online Safety Lead 2	Computing Lead	Moira Cochrane
Data Protection Lead	School Business Manager	Tracy McMahon
Data Protection Officer	Appointed Person From	Safeguarding Monitor
Supply Teacher Briefing Of Medical & SEND Information	Office Manager	Sam Ullah
Computing Subject Lead	Teacher	Moira Cochrane
Acceptable Use Forms & Use Of Digital Photos, Videos & Work Permission Forms	Office Manager	Sam Ullah & Moira Cochrane
Technical Support	Data Tools For Schools Ltd	Adam Byrnes
Software Licences & Updates	Data Tools For Schools Ltd	Adam Byrnes
Internet Firewall, Filtering & Monitoring	Smoothwall	
Internet Monitoring Reports Go To	Head Teacher	Joy Wood
	Deputy Head	Aaron Sidebottom
Anonymised Reporting (Half Termly) Of Online Safety Incidents To Governors	Deputy Head	Aaron Sidebottom
Checks (Monthly) On Smoothwall Monitoring	Business Manager	Tracy McMahon
Checks (Monthly) Of Public Social Media For Public Postings About The School & Follow Up As Necessary	Business Manager	Tracy McMahon

---

## Reporting Online Safety Concerns All Staff

**Add An Incident** on our Child Protection Online Management System (CPOMS).

**Assigned** to the Designated Safeguarding Lead Joy Wood.

**To Alert** Online Safety Lead 1 Aaron Sidebottom.

**Unless the concern involves the Designated Safeguarding Lead or the Online Safety Lead 1, in which case the concern must be reported to:**

The Chair Of Governors:  
Mr Jon Dolby

[gov.jondolby@wellington.bradford.sch.uk](mailto:gov.jondolby@wellington.bradford.sch.uk)

**And** to the Local Authority Designated Officer (LADO):  
Phone 01274 435600

[LADO@bradford.gov.uk](mailto:LADO@bradford.gov.uk)

## Schedule For Development, Monitoring And Review

This Online Safety Policy was developed by:	Moira Cochrane (Computing Lead & Online Safety Lead 2)
This Online Safety Policy was approved by the school governing body on:	17/07/2023
The implementation of this Online Safety Policy will be monitored by:	Joy Wood (Head Teacher & Designated Safeguarding Lead)  Senior Leader Aaron Sidebottom (Deputy Head & Online Safety Lead 1)  Senior Leader Catherine Berry (Assistant Head)  Safeguarding Governors: Noshaba Rashid & Mohammed Azum
The Governing Body will receive a report of anonymised details of online safety incidents from our Internet filtering and monitoring logs, generated by our Online Safety Lead 1. They will review incidents and discuss current issues.	During The Standing "Safeguarding" Agenda Item In Full Governing Body Meetings, 6 Times / Year (every half term).
Governor monitoring of the implementation of this policy will take place at regular intervals.	Annually
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next anticipated review date will be.	July 2024
Should serious online safety incidents take place, the following external persons / agencies should be informed:	The Local Authority Designated Officer (LADO)  The Police

## **Process For Monitoring The Impact Of The Online Safety Policy**

The school will monitor the impact of the policy using:

- regular review of logs of reported incidents from our filtering & monitoring reports of Internet activity (including sites visited)
- regular review of relevant Child Protection Online Management System (CPOMS) reports.

# **POLICY & 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.

## **Designated Safeguarding Lead (DSL) And Senior Leaders**

It is important to emphasise that online safety issues are safeguarding, not solely technical issues. Technology provides additional means for safeguarding issues to develop.

The Designated Safeguarding Lead, Online Safety Lead 1 and Senior Leaders 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
  - sexting (see appendix Advice For Schools: Responding To And Managing Sexting Incidents and appendix Gov.uk guidance: Sharing Nudes And Semi-Nudes)
  - inappropriate online contact with adults / strangers
  - potential or actual incidents of grooming
  - online bullying.
- 
- The Designated Safeguarding Lead has a duty of care to ensure the safety (including online safety) of members of the school community and fostering a culture of safeguarding.
  - The Designated Safeguarding Lead, Online Safety Lead 1 and Senior Leaders must 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 Designated Safeguarding Lead is responsible for ensuring that the Online Safety Leads, Senior Leaders, Technical Staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles.
  - The Designated Safeguarding Lead, Online Safety Leads and Senior Leaders will ensure that there is a system in place for monitoring.

## **Governors**

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 Governing Body who will receive regular information about online safety incidents and monitoring reports. Safeguarding Governors will:

- regularly receive (collated and anonymised) reports of online safety incidents
- annually check that the provision of online safety education provision is taking place as intended and report back to the Governing Body.

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 Leads**

The Deputy Head and Computing Curriculum Lead work together to fulfil this role.

### **Online Safety Lead 1: Deputy Head Responsibilities**

The Online Safety Lead 1 will:

- work closely on a day-to-day basis with the Designated Safeguarding Lead
- 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
- 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
- liaise with technical staff, pastoral staff and support staff (as relevant)
- provide (or identify sources of) training and advice for staff / governors / parents / carers / learners
- meet regularly with the Governing Body to review (anonymised) incidents and filtering and monitoring logs and discuss current issues
- attend relevant governing body meetings / groups
- report regularly to the Head Teacher



## **Online Safety Lead 2: Computing Curriculum Lead Responsibilities**

The Online Safety Lead 2 will:

- 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
- 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 (or identify sources of) training and advice for staff / governors / parents / carers / learners
- report regularly to the Head Teacher.

## **KS1 & KS2 Teachers Of Weekly Online Safety Lessons**

Teachers will work with the Lead for the Computing Curriculum / Online Safety to develop a planned and coordinated online safety education programme using the Project EVOLVE programme and resources.

This will be provided through:

- a programme of discrete weekly online safety lessons in all KS1 and KS2 classes
- PHSE and SRE programmes
- 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, in person, any urgent suspected misuse or problem to the Designated Safeguarding Lead and Online Safety Lead 1
- they immediately report all suspected misuse or problems to the Designated Safeguarding Lead and Online Safety Lead 1, using our Child Protection Online Management System (CPOMS) for investigation / action, in line with the school safeguarding procedures
- they identify sexting incidents, manage them and escalate appropriately (see appendix Advice For Schools: Responding To And Managing Sexting Incidents)
- all digital communications with pupils 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 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
- where lessons take place using live-streaming or video-conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies and should take note of the guidance contained in the South West Grid For Learning (SWGfL) Safer Remote Learning Resource
- 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.

## **Network Managers**

The school has a technology service provided by an outside contractor, but the school are responsible for ensuring that the provider carries out all the online safety measures that the school's obligations and responsibilities require. It is also important that the provider follows and implements school Online Safety Policy and procedures.

The network managers are 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 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 Designated Safeguarding Lead 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 (see appendix 'Technical Security Policy' for good practice).
- monitoring software / systems are implemented and regularly updated as agreed in school policies
- all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied.

## **Learners**

- are responsible for using the school digital technology systems in accordance with the Learner Acceptable Use Agreement and Online Safety Policy (this includes personal devices, where allowed)
- 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 takes every opportunity to help parents and carers understand these issues by:

- publishing the school Online Safety Policy on the school website
- providing them with a copy of our Learners' Acceptable Use Agreement
- publishing information about appropriate use of social media relating to posts concerning the school
- seeking their permissions concerning digital images etc.
- parents' / carers' meetings, newsletters, website, social media and information about national / local online safety campaigns and literature.

Parents and carers are encouraged to support the school in:

- reinforcing the online safety messages provided to learners in school.

## **Community Users**

Community users are expected to read and agree to our Community User Acceptable User Agreement, on the school sign in system, before they are provided with access to school systems.

## **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.

# ONLINE SAFETY POLICY

The school Online Safety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- allocates responsibilities for the delivery of the policy
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes / trends in technology and related behaviours
- establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world
- describes how the school will help prepare learners to be safe and responsible users of online technologies
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- is supplemented by a series of related acceptable use agreements
- is made available to staff at induction and through normal communication channels
- is published on the school website.

## Acceptable Use

The school has defined what it regards as acceptable / unacceptable use and this is shown below.

## Acceptable Use Agreements

The Online Safety Policy and acceptable use agreements define acceptable use at the school. The acceptable use agreements are communicated / re-enforced through:

- staff induction and handbook
- posters / notices around where technology is used
- communication with parents / carers
- education sessions
- the school website
- peer support.

## Guidance For Members Of The School Community:

Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to: **any illegal activity** for example:

- child sexual abuse imagery
- child sexual abuse / exploitation / grooming
- terrorism
- encouraging or assisting suicide
- offences relating to sexual images i.e. revenge and extreme pornography
- incitement to and threats of violence
- hate crime
- public order offences including harassment and stalking
- drug-related offences
- weapons / firearms offences

- fraud and financial crime including money laundering

Users shall not undertake activities that might be classed as **cyber-crime** under the Computer Misuse Act (1990) for example:

- using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access
- gaining unauthorised access to school networks, data and files, through the use of computers / devices
- creating or propagating computer viruses or other harmful files
- revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)
- disable / impair/ disrupt network functionality through the use of computers / devices
- using penetration testing equipment (without relevant permission)

The Designated Safeguarding Lead, Online Safety Lead 1 and Senior Leaders will decide whether **infringements** will be dealt with internally or by the police. Serious or repeat offences will be reported to the police. Under the Cyber-Prevent agenda the National Crime Agency has a remit to prevent learners becoming involved in cyber-crime and harness their activity in positive ways.

Users shall not undertake activities that are **not illegal but are classed as unacceptable** in school policies:

- accessing inappropriate material / activities online in a school setting including pornography, gambling, drugs (informed by the school's filtering practices and / or Acceptable Use Agreements)
- promotion of any kind of discrimination
- using school systems to run a private business
- using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school
- infringing copyright
- unfair usage (downloading / uploading large files that hinder others in their use of the internet)
- any other activity which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute.

Users shall not use **school equipment** for non-educational purposes, at school or at home including for example:

- online gaming
- online shopping / commerce
- file sharing
- social media
- messaging / chat
- entertainment streaming e.g. Netflix, Disney+
- use of video broadcasting, e.g. YouTube, Twitch, TikTok

When using **personal devices**, the school considers the following as good practice:

#### **LEARNERS:**

- learners should switch off their mobile phones when they get to the school gate and they should not turn them on again until they get to the school gate to leave at home time
- learners should hand their mobile phones in, for safe keeping, when they arrive at school, and collect them at the end of the school day

- learners should not use their own personal devices (mobile phones / smart watches / USB devices etc.) in school.

#### **STAFF, GOVERNORS & VOLUNTEERS:**

- users may bring mobile phones to school
- users shall not bring other personal devices to school e.g. cameras / tablets / gaming devices
- in areas / rooms where learners are present (including during break times, off site and residential visits) users shall keep their mobile phones out of sight and set to "silent"
- in areas / rooms where learners are present (including during break times, off site and residential visits) users shall not use their mobile phones for any purpose, including telling the time
- users shall not take photos or video footage on any mobile phone / personal device (even when the photos or videos are intended for publication beyond the school or online)
- the school acknowledges that there may be exceptional circumstances when a user may need to be contactable during the school day e.g. when a close family member is ill; at such times the user should keep their mobile phone out of sight but set to "ring" and they should step out of class into an area where learners are not present, to take any emergency calls.

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
- when communicating in a professional capacity, users should ensure that the technologies they use are officially sanctioned by the school
- any digital communication between users and learners or parents / carers (via e-mail / 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
- school e mail should not be used for personal e-mails
- users are expected to follow good practice when using personal social media to protect their own professional reputation and that of the school and its community
- users will refrain from using any form of personal social media to post about or discuss any aspect of school life
- users will follow all guidance issued, when contributing to the school's use of social media, as an official communication channel
- users should immediately report the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature, to the Designated Safeguarding Lead, and they must not respond to any such communication
- relevant policies and permissions are followed when posting information online e.g. on the school website and school social media accounts.

## **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 are made aware of the need to report online safety issues / incidents
- reports are dealt with as soon as is practically possible once they are received
- 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 Designated Safeguarding Lead and Online Safety Lead 1, unless the concern involves the Designated Safeguarding Lead or Online Safety Lead 1, in which case the complaint will be referred to the Chair of Governors and the Local Authority Designated Officer (LADO)
- where there is no suspected illegal activity, devices may be checked using the following procedures:
  - at least two 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 Designated Safeguarding Lead and Online Safety Lead 1 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
- **any urgent suspected misuse or problem** should be reported immediately, in person, to the Designated Safeguarding Lead and Online Safety Lead 1
- **all suspected misuse or problems** should be reported immediately to the Designated Safeguarding Lead and Online Safety Lead 1, using our Child Protection Online Management System (CPOMS) for investigation / action, in line with the school safeguarding procedures
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. the Local Authority Designated Officer, the police; the Professionals Online Safety Helpline, the Report Harmful Content website and the Child Exploitation And Online Protection (CEOP) website
- those involved in an incident will be provided with feedback about the outcome of the investigation and follow up actions
- follow up from an incident (or pattern of incidents) will take place (as relevant) to:
  - staff, through regular briefings
  - learners, through assemblies / lessons
  - parents / carers, through newsletters, school social media, the school website
  - governors, through regular safeguarding updates
  - local authority / external agencies, as relevant.

## **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.

## **Responding To Learner Actions**

### **Possible Incidents**

- deliberately accessing or trying to access material that could be considered illegal (see list above)
- attempting to access or accessing the school network, using another user's account (staff or learner) or allowing others to access the school network by sharing username and passwords
- corrupting or destroying the data of other users
- sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature
- unauthorised downloading or uploading of files or use of file sharing
- using proxy sites or other means to subvert the school's filtering system
- accidentally accessing offensive or pornographic material and failing to report the incident
- deliberately accessing or trying to access offensive or pornographic material
- receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act
- unauthorised use of digital devices (including taking images)
- unauthorised use of online services
- actions which could bring the school into disrepute or breach the integrity or the ethos of the school
- continued infringements of the above, following previous warnings or sanctions.

### **Possible Sanctions**

- refer to class teacher
- refer to Designated Safeguarding Lead & Online Safety Lead 1
- inform parents / carers
- remove device / network / internet access rights
- issue a warning
- further sanction, in line with behaviour policy
- refer to Local Authority / Technical Support Staff for action re filtering, etc.
- refer to local authority
- refer to police / social services

## **Responding to Staff / Volunteer / Visitor Actions**

### **Possible Incidents**



- deliberately accessing or trying to access material that could be considered illegal (see list above)
- deliberate actions to breach data protection or network security rules
- deliberately accessing or trying to access offensive or pornographic material
- corrupting or destroying the data of other users or causing deliberate damage to hardware or software
- using proxy sites or other means to subvert the school's filtering system
- unauthorised downloading or uploading of files or file sharing
- breaching copyright or licensing regulations
- allowing others to access the school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account
- sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature
- using personal e-mail / social networking / messaging to carry out digital communications with learners or parents / carers
- inappropriate personal use of the digital technologies e.g. social media / personal e-mail
- careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner
- actions which could compromise the staff member's professional standing
- actions which could bring the school into disrepute or breach the integrity or the ethos of the school
- failing to report incidents whether caused by deliberate or accidental actions
- continued infringements of the above, following previous warnings or sanctions.

## **Possible Sanctions**

- refer to Designated Safeguarding Lead & Online Safety Lead
- issue a warning
- disciplinary action
- suspension
- refer to Local Authority / Technical Support Staff for action re filtering, etc.
- refer to local authority
- refer to police

## **Online Safety Education Programme**

While regulation and technical solutions are particularly important, their use must be balanced by educating learners to take a responsible approach. The education of learners in online safety is therefore an essential part of the school's online safety provision. Learners need the help and support of the school to recognise and avoid online safety risks and develop their resilience.

The 2021 Ofsted "Review of Sexual Abuse in Schools and Colleges" highlighted the need for: "a carefully sequenced RSHE curriculum, based on the Department for Education's (DfE's) statutory guidance, that specifically includes sexual harassment and sexual violence, including online. This should include time for open discussion of topics that children and young people tell us they find particularly difficult, such as consent and the sending of 'nudes'."

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:

- using Project Evolve, a planned online safety curriculum for all year groups matched against the nationally agreed framework Education for a Connected World Framework by UKCIS/DCMS, taught in weekly lessons
- 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 other curriculum areas e.g. PHSE; SRE; Literacy etc.
- it incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- the programme 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
- learners should be helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school
- staff should act as good role models in their use of digital technologies the internet and mobile devices
- 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 that is found in internet searches
- where learners are allowed to freely 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 the period of study (any request to do so should be auditable, with clear reasons for the need)
- 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:

- mechanisms to canvass learner feedback and opinion.
- appointment of digital leaders
- the Online Safety Group has learner representation
- learners contribute to the online safety education programme e.g. peer education, digital leaders leading lessons for younger learners, online safety campaigns
- learners designing / updating acceptable use agreements
- contributing to online safety events with the wider school community e.g. parents' evenings, family learning programmes etc.

## **Staff / Volunteers**

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

- a programme of annual online safety and data protection training (E Safety & General Data Protection) will be completed by all staff
- this Online Safety Policy and its updates will be presented to and discussed by staff in staff training time
- all new staff will receive online safety and data protection training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements, including references to classroom management, professional conduct, online reputation and the need to model positive online behaviours
- the Designated Safeguarding Lead and Online Safety Leads will receive regular updates by reviewing guidance documents released by relevant organisations
- the Online Safety Leads will provide advice / guidance / training to individuals as required.

## **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 / safeguarding. This may be offered in several ways such as:

- attendance at training provided by the local authority or other relevant organisation
- 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
- opportunities for engagement with parents / carers on online safety issues through parent / carer awareness workshops
- learners who are encouraged to pass on to parents the online safety messages they have learned in lessons
- letters, newsletters, the school website
- high profile events / campaigns e.g. Safer Internet Day
- reference to the relevant web sites / publications, e.g. South West Grid For Learning (SWGfL), [www.saferinternet.org.uk/](http://www.saferinternet.org.uk/) and [www.childnet.com/parents-and-carers](http://www.childnet.com/parents-and-carers).

## **Adults And Agencies**

The school will provide opportunities for local community groups and members of the wider community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- online safety messages targeted towards families and relatives
- the school will provide online safety information via their website and social media for the wider community

## TECHNOLOGY

It is the responsibility of the school to ensure that the provider carries out all the online safety and security measures that would otherwise be the responsibility of the school. 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.

The school ensures that the technology provider is fully aware of the school Online Safety Policy and acceptable use agreements. The school has a Data Processing Agreement in place with them.

## Filtering

- the school filtering policies are agreed by senior leaders and 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 - Guide For Education Settings and Filtering Providers
- access to online content and services is managed for all users
- illegal content (e.g., child sexual abuse images) is filtered by the broadband and filtering provider
- 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 / learners)
- younger learners will use child friendly / age-appropriate search engines
- filtering logs are regularly reviewed and the school provider alerts the school to breaches of the filtering policy, which are then acted upon
- 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 South West Grid For Learning (SWGfL) Report Harmful Content site.

## Monitoring

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

- the school monitors all Internet 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
- The Designated Safeguarding Lead and Online Safety Lead 1 are 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:

- 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 The Designated Safeguarding Lead and the Online Safety Lead 1

## Technical Security

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

- 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
- there are rigorous and verified back-up routines, including the keeping of network-separated copies off-site
- all users have clearly defined access rights to school technical systems and devices; details of the access rights available to groups of users are recorded by the Network Manager and are reviewed, at least annually, by the Online Safety Leads
- all users (adults and learners) 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 systems are protected by secure passwords; the passwords must not be shared with anyone
- the master account passwords for the school systems are kept in a secure place
- the Technical Support Manager 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, as agreed
- 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 policy is in place for the provision of temporary access of 'guests', (e.g., trainee teachers, supply teachers, visitors) onto the school systems
- an agreed policy is in place regarding the extent of personal use that users (staff / learners / community users) are allowed on school devices that may be used out of school
- an agreed policy is in place that forbids staff from downloading executable files and installing programmes on school devices
- an agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices

- systems are in place that prevent the unauthorised sharing of personal data unless safely encrypted or otherwise secured.

## **Digital Media, The School Website & Social Media**

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

- ensuring that personal information is not published
- providing education / training including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues
- having clear reporting guidance, including responsibilities, procedures and sanctions
- assessment of risk, 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 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 is:

- 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
- personal accounts must not be used to associate users with / impact on the school
- personal communications which do not refer to or impact upon the school are outside the scope of this policy
- the school permits staff reasonable and appropriate access to personal social media sites during school hours i.e. during break and lunch times
- 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 pro-actively monitors the Internet for public postings about the school
- the school effectively responds 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.

## Digital And Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and learners instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and learners need to be aware of the risks associated with publishing digital images on the Internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the Internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees.

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 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
- images should only be taken on school devices; the personal devices of staff should not be used for such purposes
- in accordance with Taking Photographs: Data Protection Advice For Schools (guidance from the Information Commissioner's Office website) parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act); 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 learners 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 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 the school website or social media, particularly in association with photographs
- written 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
- 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
- learners' work can only be published with the permission of the learner and parents / carers.



## Online Publishing

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

- our school website
- social media
- online newsletters

The school website is managed by the Deputy Head. 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 images or videos are published, their identities are protected; their names are not published. Where learner work is published, their identities are protected; only their first names are published.

## 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, 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

- 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 72 hours 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
- 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:

- there is balanced professional debate about the evidence taken from 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 relevant agencies to help ensure the development of a consistent and effective local online safety strategy.

## APPENDICES

The appendices are as follows:

-  acceptable use & cloud agreement EYFS KS1 learner BACK TO BACK FORM
-  acceptable use & cloud agreement KS2 learner BACK TO BACK FORM
-  acceptable use agreement staff & volunteers BACK TO BACK FORM
-  DPO Impero DPO Service by SAMpeople
-  gdpr PACT HR policy 2022
-  governing body questions ~ online safety in schools and colleges
-  photos video and work permissions PAGES 1 & 2 BACK TO BACK TO MAKE FORM
-  safer remote learning resource
-  sexting managing incidents
-  sharing nudes and semi nudes ~ advice for education settings
-  sharing nudes and semi nudes ~ how to respond to an incident
-  use of social media ~ concern outside school ~ letter home