

**SODBURY VALE FEDERATION**

# Online Safety Policy

*Policy Number*      *SVF029*

*Version Number*      *03*

*Issue Date*      *Jan 25*

*Date of Review*      *Jan 26*



## 1 TABLE OF CONTENTS

<b>2</b>	<b><u>VERSION HISTORY</u></b>	<b>2</b>
<b>3</b>	<b><u>DEVELOPMENT MONITORING AND REVIEW</u></b>	<b>2</b>
3.1	SCHEDULE FOR MONITORING AND REVIEW	2
3.2	MONITORING	3
<b>4</b>	<b><u>SCOPE OF THE POLICY</u></b>	<b>3</b>
<b>5</b>	<b><u>ROLES AND RESPONSIBILITIES</u></b>	<b>4</b>
<b>6</b>	<b><u>ONLINE SAFETY GROUP</u></b>	<b>4</b>
<b>7</b>	<b><u>TRAINING AND AWARENESS RAISING</u></b>	<b>4</b>
<b>8</b>	<b><u>INDUCTION PROCESSES</u></b>	<b>5</b>
<b>9</b>	<b><u>TEACHING AND LEARNING</u></b>	<b>5</b>
9.1	RULES FOR KEEPING SAFE	6
9.2	EDUCATION – PARENTS / CARERS AND THE COMMUNITY	6
9.3	EDUCATION – STAFF AND VOLUNTEERS	7
9.4	TRAINING – GOVERNORS	7
<b>10</b>	<b><u>REMOTE TEACHING AND LEARNING</u></b>	<b>7</b>
<b>10</b>	<b><u>SELF-EVALUATION AND IMPROVEMENT</u></b>	<b>8</b>
<b>11</b>	<b><u>TECHNICAL ISSUES</u></b>	<b>8</b>
11.1	PASSWORD ACCESS TO SYSTEMS	9
11.2	INTERNET PROVIDER AND FILTERING	9
11.3	TECHNICAL STAFF - ROLES AND RESPONSIBILITIES	10
<b>12</b>	<b><u>USE OF DIGITAL IMAGES AND VIDEO</u></b>	<b>11</b>
<b>13</b>	<b><u>MOBILE TECHNOLOGIES</u></b>	<b>12</b>

<b>14</b>	<b>COMMUNICATIONS TECHNOLOGIES AND SOCIAL MEDIA</b>	<b>12</b>
<b>15</b>	<b>COPYRIGHT</b>	<b>13</b>
<b>16</b>	<b>DATA PROTECTION</b>	<b>13</b>
<b>17</b>	<b>TRANSFER OF DATA</b>	<b>14</b>
<b>18</b>	<b>REPORTING AND RECORDING</b>	<b>15</b>
<b>18.1</b>	<b>MANAGING INCIDENTS</b>	<b>15</b>

## 2 VERSION HISTORY

Version Number	Reason for Issue	Date of Issue
01	Initial Issue For Federation	Nov 2022
02	Review	Jan 2024
03	Review	Jan 2025

## 3 DEVELOPMENT MONITORING AND REVIEW

This Online safety policy has been developed for use within Sodbury Vale Federation and the schools within it, and will be reviewed and monitored, by the schools' online safety working groups which comprises of:

- Computing Subject Leads
- Executive Head
- A representative of teaching staff and support staff
- A governor representative and a parent representative

Consultation with the whole school community takes place through a staff meeting, School Council meeting, governors meeting, parents meeting and the school website / newsletter.

### 3.1 SCHEDULE FOR MONITORING AND REVIEW

The policy will be ratified by the full governing body (FGB). The Online safety working group will monitor the implementation of this policy annually and report on the implementation

including reported incidents to the FGB. Should serious Online safety incidents take place, the following external persons / agencies will be informed: Nick Pearce – Technical and Filtering and Jo Briscombe – Teaching and Learning Adviser ICT

### 3.2 MONITORING

The schools will monitor the impact of the policy through an analysis of:

- Logs of reported incidents and responses
- Monitoring logs of internet activity and any network monitoring data
- Monitoring information about the teaching programme and coverage within the curriculum
- Regularly checking that pupils and staff are clear about how to report incidents and respond to them
- The content of the website and twitter account is regularly monitored by governors and senior leaders to ensure that it complies with this policy and the acceptable use policies.
- Any other website, such as the school friends, that is linked to the schools name is also regularly monitored to ensure that the school is always presented accurately and professionally.

## 4 Scope of the Policy

This policy applies to **all** members of the school community within Sodbury Vale Federation (including volunteers, parents/carers, visitors and community users) who have access to or use school ICT systems inside and outside school.

The Education and Inspections Act 2006 empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is relevant to incidents, including cyber-bullying, which may take place out of school, but are linked to membership of the school. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will inform parents / carers of known incidents of inappropriate Online safety behaviour that take place out of school.

The 2011 Education Act increased these powers with regard to searching for and of electronic devices and the deletion of data and related action can only be taken over issues covered by the behaviour policy. Our behaviour policy states that, when dealing with online safety issues, electronic devices will only be searched and data deleted with parents. If parents are unavailable the device will be kept securely until a parent can meet to conduct such a search with a senior leader.

This policy should be read alongside the acceptable use policies for staff and pupils, the anti-bullying policy and the behaviour policy.

## 5 Roles and Responsibilities

These are clearly detailed in Appendix 1 for all members of the schools community.

- The governors have overall responsibility for ratifying the policy, ensuring that it is implemented and monitoring it.
- The Executive Head is responsible for ensuring the safety (including online safety) of members of the schools community, though the day to day responsibility for online safety is delegated to the Computing Leads. The Executive Head is also the designated person for child protection and is trained in online safety issues and aware of the potential for serious child protection issues to arise from sharing of personal data, access to illegal / inappropriate materials, inappropriate on-line contact with adults / strangers, potential or actual incidents of grooming and cyber-bullying.

## 6 Online Safety Group

Online Safety Group provides a consultative group that has wide representation from the schools' community, with responsibility for issues regarding online safety and monitoring the Online Safety Policy, including the impact of online safeguarding initiatives. The group will also be responsible for regular reporting to the Governing Body.

Members of the Online Safety Group will assist the Online Safety Lead (or other relevant person, as above) with:

- the production/review/monitoring of the school online safety policy/documents.
- mapping and reviewing the online safety/digital literacy curricular provision – ensuring relevance, breadth and progression
- monitoring network/internet/filtering/incident logs
- consulting stakeholders – including parents/carers and the students/pupils about the online safety provision
- monitoring improvement actions identified through use of the 360 degree safe self-review tool

## 7 Training and Awareness Raising

There is a planned programme of Online safety training for **all** staff and governors to ensure that they understand their responsibilities, as outlined in this, and the acceptable use policies. The following actions are undertaken to raise awareness:

- The Child Protection and Online Safety Leader receive regular updates through attendance at relevant training such as SWGfL and LA training

sessions and by receiving regular Online safety updates from the South Gloucestershire Traded Services.

- All staff, including support staff, receive an annual Online safety update.
- Any reported incidents and how they are addressed are discussed at staff meetings (if appropriate) and used as an opportunity to test our processes and update staff on how to deal with issues.
- The Online safety Leader provides advice/guidance and training as required to individuals and seeks LA advice on issues where appropriate.
- A training log is used to record when updates and training are delivered.

## 8 Induction Processes

- All new staff receive the Online Safety Policy as part of their induction pack.
- Parents of new reception children receive a copy of the acceptable use policy for younger children when their child starts school. There are also updates to this throughout the key stages.
- Parents of children who join school mid-year are also introduced to the acceptable use policy for their age group.

## 9 Teaching and Learning

Online safety is now a statutory part of the programme of study for all key stages. Rules and technical solutions are not infallible and we are aware that outside school children will be using unfiltered internet provision. We believe it is crucial to educate children about how to behave responsibly online and how to keep themselves and others safe. Children and young people need the help and support of the school and parents to recognise and avoid online safety risks. There is a planned and progressive scheme of work for online safety which is taught at every year group. This is based around the South Gloucestershire guidance and Digital Literacy Curriculum by SWGfL and, across the key stages, covers:

- Internet safety
- Privacy and security
- Relationships and communication
- Cyberbullying
- Information literacy
- Self image and identity
- Digital footprint and reputation
- Creative credit and copyright

The scheme of work is delivered as part of computing, PSHE and other lessons.

Regular opportunities are taken to reinforce online safety messages in all lessons and to teach pupils to be critically aware and consider the accuracy of the information they access online. Online safety messages are also reinforced through other subjects and through a

planned programme of other activities such as assemblies and events. Older pupils are taught to acknowledge the source of information and respect copyright. Pupils are helped to understand the AUP, recognise online safety risks, adopt safe practices, report any issues and keep evidence to support reporting (for older children). Staff model safe practice in use of technologies and mobile devices and guide students to appropriate sites and follow practices for dealing with unsuitable material found in internet searches. Where pupils undertake searching of the internet, staff monitor the content of the websites they are visiting. If they identify pupils who may be vulnerable, for example, who are not adopting safe practices or completing inappropriate searches this should be logged and appropriate support given to those pupils to help them understand the risks and what to do to keep safe. If there are educational reasons why a blocked site is needed for learning then staff can request that this be made available to technical staff. Where this is done this is clearly logged with reasons given for this access.

Children new to the school are provided with an overview of expectations when they start.

The following aspects also contribute to our curriculum provision:

- Coverage of learning experiences is recorded and staff check understanding when teaching about online safety.
- Annual online safety events such as Safer Internet Day are also used to raise awareness.

## 9.1 RULES FOR KEEPING SAFE

These are reinforced through the following:

- Pupils are helped to understand the student acceptable use policy and school rules for online safety and encouraged to act accordingly.
- All classes have online safety rules displayed in their classroom and staff regularly refer to these, for example, during activities where children are searching the internet for information. Rules are also displayed in other areas where ICT is used.
- Staff act as good role models in their own use of ICT.
- Staff are aware that there may be some children that are more vulnerable than others to being approached online and endeavour to ensure that these children understand the issues involved.
- Online behaviour is dealt with in accordance with our behaviour policy. There are sanctions and rewards in place for this.

## 9.2 EDUCATION – PARENTS / CARERS AND THE COMMUNITY

Parents and carers have an essential role in educating their children and monitoring their behaviour online, however they may have a limited understanding of the risks and issues

and underestimate the dangers or be unsure how to deal with them. The school aims to raise awareness and support parents through:

- Curriculum activities
- Letters and newsletters including information on any online safety issues that have been raised in school (anonymously recorded) and how to address these
- Parents / carers information evenings
- Events such as Safer Internet Day

### 9.3 EDUCATION – STAFF AND VOLUNTEERS

All staff receive regular online safety training so that they understand the risks and their responsibilities. This includes:

- A planned programme of online safety training which is regularly updated and reinforced and linked to the expectations outlined in this policy, Keeping Children Safe in Education and in the Ofsted framework.
- All new staff receive the relevant policies and expectations as part of their induction pack.
- The online safety lead receive regular updates and external training to support them to do their role.
- Policies relevant to online safety and their updates are discussed in staff meetings.
- The online safety lead provides regular guidance and training to support individuals where required.

### 9.4 TRAINING – GOVERNORS

Governors take part in online safety training and awareness raising sessions, particularly those governors who are involved with technology and safeguarding. This is offered through:

- Attendance at local authority or regional events
- Attendance at relevant staff training
- Regular newsletter information and access to website information

## 10 Remote teaching and learning

In the event of a school closure, pupils, parents, carers and teachers are reminded that the school's Child Protection and Safeguarding Policy still applies to all interactions between pupils and teachers. In that policy, there are specifically prohibited behaviours and reporting obligations to which teachers must adhere, whether they are at home, in the community or at school

- Remote learning will only take place using the Integra system.
- Staff have access to a suitable device for home use
- Staff will only use school managed or specific, approved professional accounts with learners and/or parents/carers.
- Online contact with learners and/or parents/carers will not take place outside of the operating times as defined by SLT.
- All remote lessons will be formally timetabled; a member of SLT, DSL and/or head of department is able to drop in at any time.
- Live streamed remote learning sessions will only be held with approval and agreement from the headteacher/a member of SLT.
- Students will have access to work that allows them to continue to progress while at home.
- Staff must wear suitable clothing and should be the only individual in the webinar or video.
- Any computers used should be in appropriate areas; for example, located in appropriate and suitable spaces, and where possible, be against a neutral background
- Any requests to produce a webinar or videos should be sent to the SLT , where details of how to sign in to the webinar will be shared with SLT and the Safeguarding Team.
- Staff have access to Microsoft Outlook, SIMS, CPOMS, Teams, Class Dojo and other platforms as necessary.
- Staff apply the same data protection and confidentiality safeguards as they would when working on site within their setting

## 10 Self-evaluation and Improvement

The school undertakes self-evaluation in order to inform actions to continually improve online safety provision through the following:

- Local authority safeguarding audit
- 360 degree safe online self-evaluation tool which is also used to benchmark our provision against other schools.

## 11 Technical Issues

The local authority provides technical and curriculum guidance for Online safety issues for **all** South Gloucestershire schools as well as providing direct technical support to a large number of schools.

## 11.1 PASSWORD ACCESS TO SYSTEMS

All our systems are accessed via an individual log in. Users have passwords that include upper and lower case and a number and are encouraged to change these regularly. **Users are told that passwords must never be shared for any IT system and that they are responsible for any actions taking using their log in.** Access to systems is through groups so that only the relevant group of users can access a resource.

## 11.2 INTERNET PROVIDER AND FILTERING

The South Gloucestershire school internet service is provided by Integra and this includes a filtering service to limit access to unacceptable material for all users.

Internet access is filtered for all users by South Gloucestershire School IT. Illegal content (child sexual abuse images) is filtered by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. However we are aware that no filtering is completely infallible and consequently focus on teaching pupils to keep safe through our curriculum and teaching. There are two different levels of filtering which are targeted towards different user groups. As a consequence teacher and staff users have access to some resources for teaching that are filtered for learners so as to ensure that “over blocking” does not restrict teaching.

Technical staff monitor internet traffic and report any issues to schools.

The school reports issues through logging a call to the service desk at 3838.

Any filtering requests for change and issues are also reported immediately to the South Gloucestershire technical team on 3838. Requests from staff for sites to be removed from the filtered list must be approved by the head of school or executive head and this is logged and documented by a process that is agreed by the Heads.

The schools are currently implementing a technical monitoring solution through the local authority in order to fulfil the requirements within Keeping Children Safe in Education. The iBoss solution being implemented provides the following:

- active monitoring and automatic alerts for the school to act upon, together with pro-active monitoring by Integra Schools IT to support the school by drawing attention to concerning behaviours, communications or access
- enhanced filtering integrated with the police assessed list of unlawful terrorist content, produced on behalf of the Home Office
- delegated access to the filtering system allows us to permit or deny access to specific content to support the requirement that “over blocking” does not lead to unnecessary restrictions on what can be taught relating to online teaching and safeguarding - the most severe content will always be filtered
- network level filtering which does not rely on any software on the users’ devices which could be disabled
- ability to produce reports on the websites visited by all young people and adults using our systems

- the ability for alerts to be set so that a number of people are informed when they are triggered meaning that monitoring does not need to fall into the remit of only one person which could result in issues being missed or covered up
- external alerts to people outside the school (such as safeguarding, online safety officers or IT technicians) so that monitoring is not reliant wholly on school staff and appropriate actions can be taken immediately to safeguard children and staff
- automated reporting to ensure that processes are followed without fail
- ability to log in from anywhere to see reports via web interface

### 11.3 TECHNICAL STAFF - ROLES AND RESPONSIBILITIES

Where the local authority provides technical support the “administrator” passwords for the school are not held by the school and the local authority are responsible for their security and any implications of their use. The school ensures, when working with our technical support provider that the following guidelines are adhered to.

- There are regular reviews and audits of the safety and security of school ICT systems.
- Servers, wireless systems and cabling are securely located and physical access is restricted.
- All users have clearly defined access rights to school ICT systems and are provided with a username and password by the technical support provider.
- Users are responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- An agreed policy is in place for the provision of temporary access of “guests” (e.g. trainee teachers, visitors) onto the school system. This takes the form of a generated username and password that is changed each day. This can be accessed on the admin drive.
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place regarding the downloading of executable files by users
- An agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on laptops and other portable devices that may be used out of school.

- An agreed policy is in place that forbids staff from installing programmes on school workstations / portable devices.
- An agreed policy is detailed regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school workstations / portable devices in our acceptable use agreement.
- Guest wifi access is provided through temporary log ins which expire daily.

## 12 Use of Digital Images and Video

Ease of access to technologies which take digital images and video has many benefits for learning. Taking and sharing images and video are much easier and, if not managed, this could increase the potential risk of misuse and has the potential to be used for cyberbullying. The school informs and educates users about the risks associated with digital images and these are outlined in the acceptable use policies:

- When using digital images, staff educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images including publishing their own images on social networking sites.
- Pupils should not take, use, share, publish or distribute images / video of others without their permission and staff reinforce this when appropriate.
- Written permission is obtained from parents or carers before photographs of pupils are taken. These photographs are only taken to be used for educational purposes or to promote achievements or the school.
- Staff are allowed to take digital / video images to support educational aims, but follow guidance in the acceptable use policy concerning the sharing, distribution and publication of those images.
- Images are only taken and used of individuals where there is a signed permission form in place.
- Pupils full names are not published on any online platform or school communication including the website, newsletter or twitter feed. Photographs published anywhere that include pupils are carefully selected and not used in association with pupils' full names or other information that could identify them.
- Care is always taken to ensure that pupils are appropriately dressed if images are taken and that they are not participating in any activity which might bring individuals or the school into disrepute.
- 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 as this is not covered by the Data Protection Act. However in order to protect other children and respect privacy these images should not be published or made publicly available on social networking sites. Parents / carers should also not comment on any activities involving other pupils in the digital / video images. This is clearly detailed in our acceptable use policy for parents.

- Pupils' work is only published with the permission of pupils and parents / carers.

### 13 Mobile Technologies

These might include mobile phones, tablets or any other device that has the capability of accessing the school's wireless network. The primary use of these in school is to support learning, teaching and management.

Staff and governors can gain access to wifi on personal devices through guest wifi access. This provides limited access to the internet only and not to the school network. Children are not allowed to use their personal devices in school as the school provides access to the technologies to be used for learning.

Staff are not allowed to use their personal mobile phones in school while they are teaching and any use should be restricted to times when children are not present. The only exception to this is in case of emergency, for example, during a school trip.

Staff do not use their own mobile phone to take images of children, for example, on a school trip as the school has devices available for this.

### 14 Communications Technologies and Social Media

A wide range of communications technologies have the potential to enhance learning and management. The acceptable use agreements outline how these systems should be used.

- The official school email service is used for communications between staff, and with parents/carers and students as it provides an effective audit trail. Communications are always professional in tone and content.
- Users are made aware that email communications may be monitored and what to do if they receive an email that makes them feel uncomfortable, is offensive, threatening or bullying in nature through the acceptable use policies.
- Governor communications take place through governor school e-mail accounts. Personal or sensitive information is not e-mailed but is kept on a secure online site that governors can access to via a personal user account.
- Personal email addresses, text messaging, public chat and social networking programmes are not to be used for communications with parents/carers and children.
- An online secure platform is used for pupil learning and this includes secure access to communications tools so that children can learn about these within a limited environment.

- The school uses the school website and Class Dojo to update parents on news and events and this is managed and monitored by a named member of staff who approves content and monitors use of the account.
- Personal information is also not posted on the school website and only official email addresses are listed for members of staff. The web site is the ultimate responsibility of the executive head with the support of the head of school and office staff.
- Guidance on personal use of social media and mobile devices is included in the staff, parent and pupil acceptable use policies including clear reporting mechanisms. Training is provided for staff and risks, reporting and issues around social networking forms part of the learning for pupils.
- Staff ensure that no reference is made in social media to pupils, parents or other staff and do not engage in online discussions on personal matters about any member of the school community
- Personal opinions are not attributed to the school
- Security settings on personal social media profiles are regularly checked to minimise risk
- Staff personal use of social media where it does not relate to the school is outside the scope of the policy but it should be made clear that the member of staff is not communicating on behalf of the school. If staff come across communications that might bring the school into disrepute in their personal communications they should not get involved, refer the publisher to relevant complaints procedures and report the issue.
- The online safety lead pro-actively monitors the Internet for postings about the school through the use of BOOST which includes a reputation alert.

## 15 Copyright

The Schools Business Manager is responsible for making sure that the software licence audit is regularly updated and also making regular checks to ensure the number of software installations matches the licences held. Where there are insufficient licences this could breach the Copyright Act which may lead to fines or unexpected additional license costs.

## 16 Data Protection

Personal Data is defined as any data which relate to a living individual who can be identified from the data. This includes opinion about the individual. Sensitive Personal Data about a person includes information about their racial or ethnic origin, political opinions, their religious beliefs or other beliefs of a similar nature, whether they are a member of a trade union and their physical or mental health or condition.

Personal data is recorded, processed, transferred and made available according to the Data Protection Act 1998 and is:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure and only transferred to others with adequate protection

## 17 Transfer of Data

Whenever possible secure online storage is used to ensure that documents do not need to be transferred to limit the risk. We ensure that data is stored in accordance with the requirements laid down by the Information Commissioner's Office and within the EU. This also applies to cloud storage used.

The school ensures that:

- It holds the minimum personal data necessary to enable it to perform its function and does not hold it for longer than necessary for the purposes it was collected for.
- The data held is accurate, up to date and inaccuracies are corrected as quickly as possible.
- All personal data is fairly obtained in accordance with our "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing" as outlined in the policy on the South Gloucestershire IMS Traded Services web site.
- Personal and sensitive data relating to pupils or staff is not e-mailed as this is not secure.
- Personal data including assessment data is transferred using secure file transfer.
- Where information does need to be transferred between devices then encrypted memory sticks are used.
- It has clear and understood arrangements for the security, storage and transfer of personal data
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- There is a Senior Information Risk Officer (SIRO) and Information Asset Owner (IAOs) in place.
- Risk assessments are regularly carried out.
- Data subjects have a right to access their data and there are clear procedures for this.
- There are clear and understood policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from information risk incidents.

- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties.
- Only cloud storage that meets the requirements laid down by the Information Commissioner's office is used to store personal data.
- The staff acceptable use policy clearly defines the data protection measures that staff should take and how data can be securely stored and deleted.

Staff ensure that they

- Take care to ensure safe keeping of personal data and minimise the risk or loss or misuse
- Use personal data only on secure password protected computers and devices and log off at the end of every session
- Transfer data using encryption and secure password protected devices. Where personal data is stored on removable media:
  - The data is encrypted and password protected
  - The device is password protected
  - The device has approved virus and malware checking software
  - The data is securely deleted from the device once finished with.

## 18 Reporting and Recording

There are clear reporting mechanisms in place for online safety incidents and all staff are regularly reminded of these and fully aware of their responsibilities to follow up any reported issues.

Staff should report online safety issues are reported to the Online Safety Lead. If these include allegations of bullying then the anti-bullying policy is followed. Issues which may impact on the well-being and safety of a child are reported directly to the Child Protection Lead and Child Protection procedures are followed. Issues impacting on staff or to the detriment of the school should be reported to the Executive head or to the Chair of Governors if the executive head is absent or the accusation involves the executive head. Pupils are encouraged to report any incidents to an adult whether it relates to themselves or a friend. We encourage children to take responsibility for protecting each other.

### 18.1 MANAGING INCIDENTS

In the event of suspicion of an infringement of policy then all the following steps should happen.

- More than one senior member of staff should be involved in investigating to protect possible future accusations.
- Use a computer that will not be used by young people which could be taken off site by the police if required.
- Ensure staff have internet access to investigate but that sites and content are closely monitored and recorded.

- Record the URL of any site containing alleged misuse and the nature of the content causing concern. It may be useful to record and store screenshots of the content by printing them, signing them and attaching them to the record. Except for child abuse images as this would constitute an offence.
- Once the investigation is complete the investigating group should identify the appropriate response in line with policies which may internal procedures, involvement of LA or police.

#### Reporting to the police

- If the content being reviewed includes images of child abuse then monitoring should be stopped and the police informed immediately. Other incidents to be referred to the police are
  - incidents of 'grooming' behaviour
  - the sending of obscene materials to a child
  - adult material which potentially breaches the Obscene Publications Act
  - criminally racist material
  - promotion of terrorism or extremism
  - other criminal conduct, activity or materialsIn any of the above, isolate the computer involved as any change to its stage may hamper a police investigation.

If issues could be a result of problems with infrastructure or may affect it then the technical support provider is informed immediately (for South Gloucestershire support 3838).

If access to an unsuitable site is reported then the Online Safety lead will alert the technical support team by ringing 3838 to ensure that this is blocked. Serious incidents are escalated to local authority staff for advice and guidance

Nick Pearce – infrastructure, technical and filtering – 01454 863838

Jo Briscoombe – curriculum and policy – 01454 863349

Jon Goddard – LADO allegations against staff and volunteers – 01454 868508

Access and response team (ART) – safeguarding / child protection concerns - 01454 866000 (Monday to Friday) and 01454 615165 (Out of hours/Weekends)

For incidents affecting school staff the Professionals Online Safety Helpline is contacted for advice if necessary on [helpline@saferinternet.org.uk](mailto:helpline@saferinternet.org.uk) or 0844 381 4772.

Any reported incidents are logged in the online safety log and followed up in accordance with the relevant policy depending on the issue. The response is also logged and serious issues are followed up after an interval of time to ensure that they are fully resolved.

Where appropriate school newsletters and the website are used to provide guidance to staff following an incident in order to prevent further incidents happening.

There are defined sanctions in place for any breaches of the acceptable use policies.

### Appendix 1: Roles and Responsibilities

Role	Responsibility
Governors	<p>Approve and review the effectiveness of the online safety policy and acceptable use policies</p> <p>Online safety governor works with the online safety leader to carry out regular monitoring of online safety incident logs, filtering, changes to filtering and then reports to governors.</p>
Executive Head, Head of School and Senior Leaders:	<p>Duty of care to ensure the safety (and online safety) of the school community. The Executive head and at least one other member of SLT should know the procedure to be followed in the event of a serious online safety allegation being made against a member of staff.</p> <p>Ensure that all staff receive suitable CPD to carry out their Online safety roles.</p> <p>Ensure that there is a system in place for monitoring and support of those who carry out the internal online safety role.</p> <p>Inform the local authority about any serious Online safety issues including filtering. Ensure that the school infrastructure / network is safe and secure and that policies and procedures approved within this policy are implemented.</p>
Online safety Leader:	<p>Lead the online safety working group and deals with day to day online safety issues Lead role in establishing / reviewing online safety policies / documents and checking links to other policies</p> <p>Ensure all staff are aware of the procedures to follow if there is an online safety incident</p> <p>Provide and/or broker relevant training and advice for all school staff</p> <p>Attend updates and liaise with the LA online safety staff and technical staff</p> <p>Receives reports of online safety incidents and keeps the incident log updated Meet with online safety governor to regularly to discuss issues, review the incident log and filtering / changes to filtering log</p> <p>Report regularly to SLT</p> <p>Develop an online safety teaching programme to deliver the statutory programme of study. Monitor online safety teaching to ensure this is being delivered and is having an impact on pupils' understanding.</p>
Child Protection Safeguarding Lead	<p>Have received training in online safety issues and know the potential for child protection and safeguarding issues to arise from sharing personal data, access to illegal // inappropriate materials, inappropriate online contact with strangers, potential or actual incidents of grooming and cyber-bullying.</p>
Curriculum Leaders	<p>Ensure online safety is appropriately reflected in teaching programmes where relevant eg anti bullying, English publishing and copyright and is reflected in relevant policies.</p>

<p>Teaching and Support Staff</p>	<p>Ensure they have an up to date awareness of school online safety issues, policies and practices.                  Have read, understood and signed the Staff Acceptable Use Agreement (AUP)                  Act in accordance with the AUP and Online safety policy                  Report any suspected misuse or problem to the headteacher / online safety leader. In the event that the incident involves the headteacher report to the governor responsible for safeguarding.                  Only communicate with pupils / parents / carers professionally through official school systems                  Ensure online safety issues are embedded in the curriculum and other activities                  Ensure pupils follow the online safety rules                  Ensure that the school programme of study for online safety is delivered through their teaching                  Monitor ICT activity in lessons, extra curricular and extended school activities Deliver the scheme of work for online safety and ensure children have a good understanding of what they are being taught.                  Monitor use of digital technologies (mobile devices and cameras etc) in lessons and other school activities where their use if allowed and implement policies about their use. Ensure that students are guided to appropriate sites in pre-planned internet use, that they are aware of how to search more safely and that any unsuitable material that is accessed is dealt with according to school policy.                  Immediately report any issues in accordance with school policy.</p>
<p>Students / pupils</p>	<p>Use schools systems in accordance with the pupil acceptable use policy                  Practice age-appropriate safe searching in order to reduce access to unsafe material. Understand how to report online safety issues and do this immediately when an issue arises                  Know and follow the policies on use of mobile devices and cameras including taking images.                  Understand the importance of using technologies safely outside school and know that the policy covers actions out of school that are related to their membership of the school. Help their friends to keep safe by pointing out any risks and what they could do about them.</p>

<p>Parents and carers</p>	<p>Read the school guidance about online safety in the newsletter and on the website and take appropriate action if required to keep their child safe.                  Agree to endorse the Pupil Acceptable Use Policy                  Ensure that their child / children follow appropriate acceptable use rules at home                  Discuss online safety issues with their child / children and monitor their home use of ICT systems (including mobile phones and games devices) and the internet                  Access the school website / online platform in accordance with the relevant school Acceptable Use Policy.</p>
---------------------------	--

	<p>Keep up to date with issues through school updates and attendance at events</p> <p>Ensure they follow the school policy on taking digital and video images at school events. Ensure their children following rules on appropriate use of childrens' own devices in school</p> <p>Report any online safety issues that could impact on safeguarding of any children or learning in school so that the school can put in place appropriate measures and use these to inform any changes to teaching.</p>
<p>Technical Support Provider</p>	<p>Ensure the school's ICT infrastructure is secure and is not open to misuse or malicious attack</p> <p>Ensure that the school meets Online safety technical requirements of the LA. Ensure users may only access the school network through an enforced password protection policy, where passwords are regularly changed</p> <p>Ensure that filtering is robust is blocking but does not inhibit learning and teaching</p> <p>Keep up to date with online safety technical information and update others as relevant Ensure use of the network is regularly monitored in order that any misuse / attempted misuse can be reported to the head teacher / online safety leader for investigation / action / sanction.</p> <p>Ensure monitoring software / systems are implemented and updated</p> <p>Ensure all security updates / patches are applied (including up to date anti-virus definitions, windows updates) and take action to prevent spyware and malware.</p>
<p>Community Users</p>	<p>Agree to follow the AUP before being provided with access to school systems.</p>