

## Online Safety and Use of Social Media Policy

| Date           | Review Date    | Leader     | Nominated Governor |
|----------------|----------------|------------|--------------------|
| September 2026 | September 2027 | Martin Yeo | Peter Murley       |

This online safety policy has been developed by Online Safety Leader (Martin Yeo) in conjunction with:

- Headteacher – Laura Oakes
- Staff – including teachers, support staff, technical staff
- Computing Technician – Alex Chedney
- Governors (including Safeguarding and Online Safety Governor) – Peter Murley
- Parents and carers
- Community users

### 1) Scope of the Policy

This policy applies to all members of the *school* community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school digital technology systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers 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 pertinent to incidents of online-bullying or other online safety incidents covered by this policy, which may take place outside of the *school*, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The *school* will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

### 2) Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

#### Governors

*Governors* are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the *Governors* receiving regular information about online safety incidents and monitoring reports. A member of

the *Governing Body* has taken on the role of *Online Safety Governor*. The role of the *Online Safety Governor* will include:

- regular meetings with the Online Safety leader
- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs
- reporting to the Governing Body

### **Headteacher and Senior Leaders**

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, although the day-to-day responsibility for online safety will be delegated to the Online Safety Lead.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents).
- The Headteacher is responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher and Senior Leaders will monitor and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

### **Online Safety Lead**

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety development.
- meets with *Online Safety Governor* to discuss current issues, review incident logs and filtering/change control logs
- attends relevant meetings of the *Governing Body*
- reports regularly to the Headteacher and SLT

### **Technical staff**

Those with technical responsibilities are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local Authority online safety guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that 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

- that the use of the networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher and Senior Leaders; Online Safety Lead for investigation.
- that monitoring software/systems are implemented and updated as agreed in school policies

### **Teaching and Support Staff**

Are responsible for ensuring that:

- they have an up-to-date awareness of online safety matters and of the current school online safety policy and practices
- they have read, understood and signed the staff acceptable use policy
- they report any suspected misuse or problem to the Headteacher/Senior Leader/Online Safety Lead for investigation.
- all digital communications with students/pupils/parents/carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online Safety Policy and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

### **Designated Safeguarding Lead**

Should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding 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
- online-bullying

### **Pupils**

- are responsible for using the school digital technology systems in accordance with the student/pupil acceptable use agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of the internet, mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the *school's/academy'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 internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, social media and information about national/local online safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website/Learning Platform and on-line student/pupil records
- their children's personal devices in the school (where this is allowed)

## **3) Education and Training**

### **Pupils**

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety/digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

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

- A planned online safety curriculum should be provided as part of Computing/PHSE/other lessons and should be regularly revisited.
- The content of the Online Safety Curriculum will be updated in line with emerging online risks.
- Extra online safety lessons may be planned in to the curriculum in response to incidents where pupils have been exposed / exposed themselves to an online risk.
- Key online safety messages should be reinforced as part of a planned programme of assemblies.
- Pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Pupils should be helped to understand the need for the pupil 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 pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in 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 can request that the Technical Staff (or other relevant designated person) can temporarily remove 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.

### **Parents/carers**

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

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

- Curriculum activities
- Letters, newsletters, web site, Learning Platform
- Parents/carers evenings/sessions
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant web sites/publications e.g. [swgfl.org.uk](http://swgfl.org.uk), [www.saferinternet.org.uk/](http://www.saferinternet.org.uk/), <http://www.childnet.com/parents-and-carers>

### **Education & Training – Staff/Volunteers**

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- Online safety and cyber-security training will be delivered annually to all staff. The content of this training will be updated in line with government guidance.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements.
- The Online Safety Lead (will receive regular updates through attendance at external training events (e.g. from SWGfL/LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This online safety policy and its updates will be presented to and discussed by staff during a professional development meeting.
- The Online Safety Lead provide advice/guidance/training to individuals as required.

### **Governors**

Governors should take part in annual online safety training sessions, particularly if they are members of any group involved in technology/online safety/health and safety/safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority.
- Participation in school training sessions for staff or parents (this may include attendance at assemblies and or/lessons).

## **4) Maintenance of Technical Infrastructure and Equipment,**

The school will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

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 must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All staff members will use their own individual usernames and passwords to access the school server.
- Pupils will be provided with their own username and secure passwords to allow them to access online learning resources. Class teachers will keep an up to date record of users and their usernames and passwords.
- Users are responsible for the security of their username and password.
- When accessing the school network, pupils will only have access to files and information that are relevant to them. They will not have access to any confidential or inappropriate information.
- The “master/administrator” passwords for the school systems, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place.
- Subject leaders are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc. 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 devices are protected by up to date virus software.
- Only software agreed by the school’s Online safety lead may be installed on school devices.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

## **5) Filtering and Monitoring**

### **What is filtering and monitoring?**

Filtering and monitoring systems are used to keep pupils safe when using the school’s IT system.

**Filtering systems:** block access to harmful sites and content.

**Monitoring systems:** identify when a user accesses or searches for certain types of harmful content on school devices (it doesn’t stop someone accessing it). Our school is then alerted to any concerning content so we can intervene and respond.

**Roles:**

### **Responsibility of the Head Teacher / Designated Safeguarding Lead and Senior leadership team (SLT):**

- Buying-in the filtering and monitoring system your school uses
- Ensuring that all of the relevant filtering and monitoring standards are met.
- Identify any risk that are specific to the school e.g. when, where and how technology is used to access the internet.

- Deciding and documenting what is blocked or allowed, and why, including gen-AI sites.
- Reviewing the effectiveness of the filtering and monitoring system (at least annually) making sure that incidents are urgently picked up, acted on and outcomes are recorded
- Checking relevant monitoring and filtering reports that have been created by the IT technician.
- Responding to safeguarding concerns identified by filtering and monitoring
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Making sure staff:
  - Understand their role
  - Are trained appropriately
  - Follow policies, processes and procedures
  - Act on reports and concerns

### **Responsibility of the IT Technician**

- Offer advice on which filtering and monitoring system the school should buy in to.
- Offering technical assistance on the use of the filtering and monitoring system.
- Providing filtering and monitoring reports
- Maintaining the filtering and monitoring system

### **The Responsibilities of the Governing body**

- To have overall strategic responsibility for filtering and monitoring and will need assurance from you that your school is meeting the standards.
- To provide challenge and support as required.
- The chair of governors will be responsible for making sure filtering and monitoring standards are met

### **The Responsibilities of All Staff include:**

- monitoring what is on pupils' screens
- understanding how to report safeguarding and technical concerns, or failures to the monitoring and filtering system, including when unreasonable restrictions affect teaching and learning or administrative tasks.
- providing clear guidelines to pupils when they are accessing the internet.

### **The School's Filtering System**

The school uses a combination of **Sophos UTM Firewall and Senso Filtering and Monitoring** for its filtering and monitoring system. These products meet all the requirement set out by KCSIE 2026. It allows the school to create reports using specific date and time windows and filter categories e.g. pornography or extremism. It also allows the school to identify user details including IP addresses and specific search keywords used.

Internet access is filtered for all users. Illegal content is filtered by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated.

The IT Technician creates weekly filtering reports using the filtering system. These are emailed to the school's head and deputy head teacher and reviewed and discussed accordingly. Any relevant actions as a result are taken.

## **Reviewing the Effectiveness of the School's Monitoring and Filtering System**

The school will review the effectiveness of the filtering and monitoring system using a filtering and monitoring check list, **annually**, or when:

- a new safeguarding risk has been identified
- there is a change in our working practices (such as allowing remote access, or staff to bring their own devices)
- a new technology is introduced
- there are major software updates
- there are changes to the technical configuration of the network and devices

Incidents where the filtering system has been breached and as a result, pupils have been exposed to inappropriate content are always logged in the "Online Safety Incident Log". An example of this log can be found in the appendix 2.

### **Education/Training/Awareness**

Pupils will be made aware of the importance of filtering systems through the online safety education programme will also be warned of the consequences of attempting to subvert the filtering system. Staff users will be made aware of the filtering systems.

Parents will be informed of the school's filtering policy through the acceptable use agreement and through online safety awareness sessions.

## **5) Mobile Technologies**

### **What are Mobile Devices?**

Mobile technology devices may be school owned/provided or personally owned and might include: smartphones, tablets, notebooks/laptops or other technology that usually has the capability of utilising the school's wireless network. These devices then has access to the wider internet and other cloud-based services such as email and data storage.

### **Mobile Devices Belonging to Pupils**

Mobile phones and other smart technology with similar functionality e.g. smartwatches are not used, seen or heard by pupils during the school day, including lessons, social times and school-organised activities, unless the headteacher has agreed to a specific educational, medical, SEND or safeguarding exception. This establishes a phone-free school day.

Where a pupil needs a phone for travel safety, it must be switched off and handed to the school office for secure keeping at the start of the day, then collected at the end of the day. The school is not responsible for personal devices brought onto the premises except where liability arises in law.

Unauthorised devices may be confiscated. Parents will be informed and may be required to collect the device. Repeated or serious misuse, including recording, photographing, bullying, harassment, sharing harmful material or accessing inappropriate content, is addressed under behaviour, safeguarding and online safety procedures.

Pupils will be taught the risks that are associated with the use of mobile phones, both in school and more broadly, to make sure they understand the decision to prohibit

the use of mobile phones throughout the school day. These risks can include a loss of focus in lessons, classroom disruption and an increase in bullying. Pupils will be encouraged to see a mobile-phone free environment as desirable and valuable.

Pupils in EYFS, Key Stage 1 and Key Stage 2 are not permitted to bring mobile phones on school trips, educational visits or residential visits. Communication between pupils and parents/carers during visits will normally take place through school staff and the designated visit leader. Parents/carers should contact the school office if they need to pass information on to their child during a visit.

Any exception must be agreed in advance by the visit leader and/or Headteacher. Exceptions will only be considered on an individual basis and where there is evidence and professional recommendation e.g. medical need or a safeguarding requirement. Where a pupil is permitted to bring a mobile phone, principles align to this policy and a pupil mobile phone permission form must be completed. The phone must remain switched off and securely stored unless otherwise instructed by a member of staff. Pupils must not take photographs, videos or audio recordings of pupils, staff or members of the public. Any device used in breach of this policy may be confiscated by the visit leader.

Staff and Parent volunteers accompanying visits must:

Follow this policy.

- Not use personal phones while supervising pupils except in an emergency.
- Not photograph or record pupils using personal devices.
- Not contact other parents/carers directly regarding pupils during the visit.

### **School Owned Mobile Devices Used by Pupils**

- School mobile devices will be used to support and enhance the curriculum. Members of staff will only use Apps which are age appropriate and which have been ratified by a member of the SLT.
- When not being used, school mobile devices, used by children, should be stored securely (in charging units if available).
- Teaching about the safe and appropriate use of mobile technologies is an integral part of the school's online safety education programme.

### **The Use of Mobile Devices by Members of Staff**

Staff (including volunteers, contractors and anyone else otherwise engaged by the school) are not permitted to use their personal mobile phone during the school day, while pupils are present, during contact time. Use of personal mobile phones must be restricted to non-contact time, and to areas of the school where pupils are not present (such as the staffroom).

There may be circumstances in which it's appropriate for a member of staff to have use of their phone during contact time, for personal reasons. For instance (this list is non-exhaustive):

- For emergency contact by their child, or their child's school
- In the case of acutely ill dependents or family members

The headteacher will decide on a case-by-case basis whether to allow for special arrangements.

If special arrangements are not deemed necessary, school staff can use the school office number as a point of emergency contact.

Staff must not use their personal mobile phones to process personal data, or any other confidential school information, including entering such data into generative artificial intelligence (AI) tools such as chatbots (e.g. ChatGPT and Google Gemini).

Staff must not use their personal mobile phones to take photographs or recordings of pupils, their work, or anything else that could identify a pupil. If it's necessary to take photos or recordings as part of a lesson, school trip, activity, this must be done using school equipment.

In some circumstances, it may be appropriate for staff to use personal mobile phones or a similar device during the school day in front of pupils for work. Such circumstances may include, but are not limited to:

- Use of multi-factor authentication
- Emergency evacuations
- Supervising off-site trips
- Supervising residential visits

Longleaze Primary School has a school mobile phone, which is taken on school trips and provided to the named trip leader. However, in exceptional circumstances it may be necessary for a staff member to use their personal mobile phone when supervising residential visits or school trips. If in this circumstance, the staff member must advise the headteacher.

In these circumstances, staff will:

Use their mobile phones in an appropriate and professional manner, in line with our staff code of conduct

Not use their phones to take photographs or recordings of pupils, their work, or anything else that could identify a pupil

Refrain from using their phones to contact parents/carers unless absolutely necessary e.g. in the case of an emergency or outside of the school day when contact cannot be made by the school office. Staff should retain/block their own personal number unless the situation is an emergency.

### **School Owned Devices Used by Staff**

- The school may also allocate school owned mobile devices (including laptops) to members of staff to support them in their teaching role.
- These devices will be included on the school's asset register and members of staff will sign for them after they have been allocated. When a member of staff leaves the school, these mobile devices will be returned.
- All school mobile devices (including laptops), used by members of staff, will be password protected.
- Members of staff may take mobile devices home with them, but their primary purpose should be educational.
- Members of staff should use school owned mobile devices responsibly and store them securely when not being used.
- The use of school owned mobile devices for inappropriate or illegal activities could lead to disciplinary or legal action.

- Members of staff may use school allocated mobile devices for the taking of photos or videos of children for educational purposes. They will only use work-provided equipment for this purpose.
- Wherever possible, contractors will be asked to carry out maintenance outside of school hours. Where essential maintenance or emergency repair is required in teaching areas during school hours, all contractors will be supervised to comply with this policy.
- On school trips, teachers may use their own mobile phones to contact each other or to communicate with school. If a member of staff needs to contact a parent / carer while on a school trip, a school mobile phone (password protected) will be used.
- Communication between parents/carers and members of staff within or outside of the school should only take place via an approved school email account or a school telephone or mobile device, unless under the direction of the headteacher e.g. during residential.

## 6) Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students/pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils 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.

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website/social media/local press.
- 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 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 *students/pupils* in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students/pupils must not take, use, share, publish or distribute images of others without their permission

- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

## **7) Data Protection**

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

### **The school must ensure that:**

- it has a Data Protection Policy.
- it implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records.
- it has paid the appropriate fee Information Commissioner's Office (ICO) and included details of the Data Protection Officer (DPO).
- it has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest. The school may also wish to appoint a Data Manager and Systems Controllers to support the DPO
- it has an 'information asset register' in place and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it
- the information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded
- it will hold only the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for. The school should develop and implement a 'retention policy' to ensure there are clear and understood policies and routines for the deletion and disposal of data to support this. personal data held must be accurate and up to date where this is necessary for the purpose it is processed for. Have systems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
- it 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)
- procedures must be in place to deal with the individual rights of the data subject, e.g. one of the 8 data subject rights applicable is that of Subject Access which enables an individual to see to have a copy of the personal data held about them (subject to certain exceptions which may apply).
- data Protection Impact Assessments (DPIA) are carried out where necessary. For example, to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier (this may also require ensuring that data processing clauses are included in the supply contract or as an addendum)
- IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring fenced from systems accessible in the classroom/to learners

- it has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.
- it understands how to share data lawfully and safely with other relevant data controllers.
- it reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach in accordance with UK data protection 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.
- if a maintained school, it must have a Freedom of Information Policy which sets out how it will deal with FOI requests.
- all staff receive data protection training 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.

### **The Storage of Personal Data**

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

- data must be encrypted and password protected.
- device must be password protected.
- device must be protected by up -to-date virus and malware checking software
- data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.
- staff take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- staff are able to recognise a possible breach, understand the need for urgency and know who to report it to within the school

Where personal data is stored or transferred on mobile or other devices (including USBs) these must be encrypted and password protected. The school will not transfer any school personal data to personal devices except as in line with school policy. The school will access personal data sources and records 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.

## **8) Communications**

A wide range of rapidly developing communications technologies have the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

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

- The official staff and class email accounts are regarded as safe and secure and are monitored. Staff should therefore use only these email accounts to communicate with others, when in school. Staff will use class email accounts to communicate with parents and carers and staff email accounts to communicate with other professionals.
- Users must immediately report, to the headteacher, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

- Any digital communication between staff and pupils or parents/carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class/group email addresses may be used by pupils to communicate. The content of these emails will be closely monitored and the recipients of these emails will be selected by the class teacher
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

## 9) Use of Social Media

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of pupils, the school and the individual when publishing any material online. Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012'. Ofsted's online safety inspection framework reviews how a school protects and educates staff and pupils in their use of technology, including the measures that would be expected to be in place to intervene and support should a particular issue arise. Schools/academies are increasingly using social media as a powerful learning tool and means of communication. It is important that this is carried out in a safe and responsible way.

All schools, academies, MATs and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies, MATs and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the *school* or local authority/MAT liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through social media by:

- Ensuring that personal information is not published on any form of social media.
- Providing clear reporting guidance in situations when protocols are breached
- Providing guidance to staff on the acceptable use of social media and the associated risks and measure that should be put in to place to mitigate these risks.

### **School staff should ensure that:**

- no reference is made on social media to pupils, parents/carers or school staff
- they do not engage in online discussion on personal matters relating to members of the school community
- they do not make comments or post content that reflects the school in a negative way
- their own personal opinions should not be attributed to or link to the *school in any way*.

- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
- they do not use social media to contact, “follow” or “friend” any pupils who are currently attending the school or allow these pupils to “follow” or “friend” their own social media accounts.
- must not give their personal contact details to parents/carers or pupils, including by connecting through social media and messaging apps.
- must avoid publicising their contact details on any social media platform or website, to avoid unwanted contact by parents/carers or pupils. (Staff Behaviour Policy)

Staff are permitted to use personal social media accounts during their own free time but access to these accounts must be through personal devices in an area of the school designated to staff only e.g. the staffroom. Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

***Social media accounts are used to promote the school and to communicate with members of its community. In this case:***

- *All content will be posted via a school administrator who will monitor its quality and appropriateness.*
- *Staff will be provided with guidance on what types of images and content should be posted on social media sites.*
- *Social media pages are regularly monitored by the school’s administrators.*
- The school will respond to comments made by others on its social media accounts in a respectful and professional manner.
- Any abuse and misuse of these social media accounts by any members of the school community is reported to the Headteacher or the Chair of Governors. These incidents may be dealt with under the school’s disciplinary procedures.

## **10) Dealing with Unsuitable/inappropriate Activities**

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

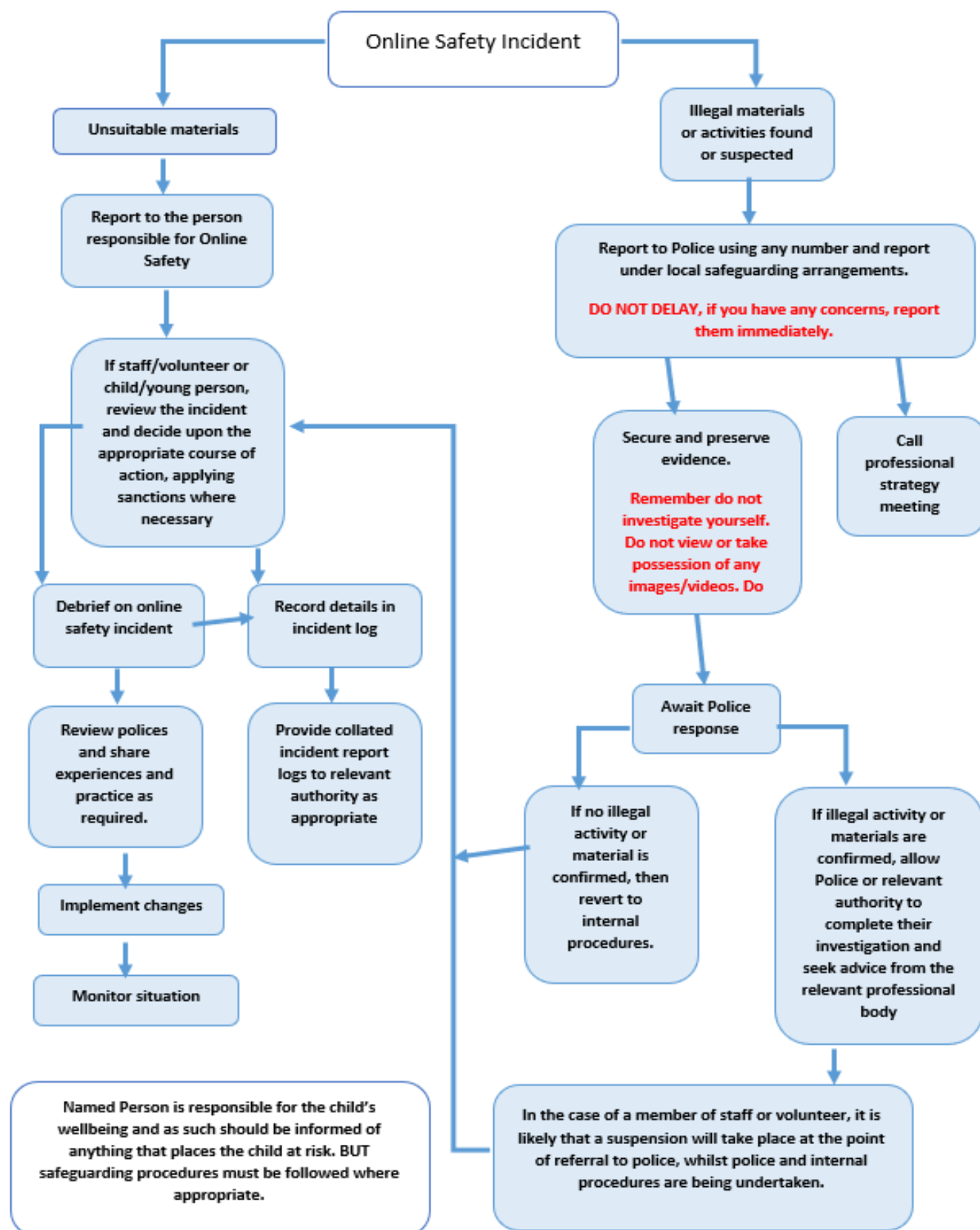
The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in/or outside the school when using school equipment or systems. The school policy restricts usage as follows:

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Acceptable | Acceptable at certain | Acceptable for | Unacceptable | Unacceptable and illegal |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|-----------------------|----------------|--------------|--------------------------|
| Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978                                                                                                                                                                                                                                                                                                                                                                                                                                         |            |                       |                |              | X                        |
| Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.                                                                                                                                                                                                                                                                                                                                                                                                                                                               |            |                       |                |              | X                        |
| Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008                                                                                                                                                                                                                                                                                                                                                                                                                |            |                       |                |              | X                        |
| Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986                                                                                                                                                                                                                                                                                                                                                                                                                                   |            |                       |                |              | X                        |
| Pornography                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |            |                       |                | X            |                          |
| Promotion of any kind of discrimination                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |            |                       |                | X            |                          |
| Threatening behaviour, including promotion of physical violence or mental harm                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |            |                       |                | X            |                          |
| Promotion of extremism or terrorism                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |            |                       |                | X            |                          |
| Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute                                                                                                                                                                                                                                                                                                                                                                                                                                       |            |                       |                | X            |                          |
| Activities that might be classed as cyber-crime under the Computer Misuse Act:<br>Gaining unauthorised access to school networks, data and files, through the use of computers/devices<br>Creating or propagating computer viruses or other harmful files<br>Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)<br>Disable/Impair/Disrupt network functionality through the use of computers/devices<br>Using penetration testing equipment (without relevant permission) |            |                       |                |              | X                        |
| Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school                                                                                                                                                                                                                                                                                                                                                                                                                                                            |            |                       |                | X            |                          |
| Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)                                                                                                                                                                                                                                                                                                                                                                                                                            |            |                       |                | X            |                          |
| Unfair usage (downloading/uploading large files that hinders others in their use of the internet)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |            |                       |                | X            |                          |
| Using school systems to run a private business                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |            |                       |                | X            |                          |
| Infringing copyright                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |            |                       |                | X            |                          |

|                                        |   |   |   |   |  |
|----------------------------------------|---|---|---|---|--|
| On-line gaming (educational)           |   |   | X |   |  |
| On-line gaming (non-educational)       |   | X |   |   |  |
| On-line gambling                       |   |   |   | X |  |
| On-line shopping/commerce              |   |   |   | X |  |
| File sharing                           | X |   |   |   |  |
| Use of social media                    |   | X |   |   |  |
| Use of messaging apps                  |   | X |   |   |  |
| Use of video broadcasting e.g. YouTube |   | X |   |   |  |

## 11) Responding to Incidents of Misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities:



## Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.

## Other Incidents

All members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

### **In the event of suspicion, all steps in this procedure will be followed:**

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should 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 (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
  - Internal response or discipline procedures
  - Involvement by the Local Authority
  - Police involvement and/or action
- **If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
  - 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
  - offences under the Computer Misuse Act (see User Actions chart above)
  - other criminal conduct, activity or materials
  - Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the *school* and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

## **12) School Actions & Sanctions**

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.

### **Possible Sanctions or consequences for members of staff may include:**

- Reporting to Headteacher or SLT member
- Reporting to Local Authority (LADO)
- Reporting to Police
- Reporting to Technical Support Staff for action re filtering etc.
- Warning
- Suspension
- Disciplinary action

### **Possible Sanctions or consequences for pupils may include:**

- Reporting to class teacher/
- Reporting to Headteacher or police
- Reporting to Police
- Reporting to technical support staff for action re filtering/security etc.
- Informing parents/carers
- Removal of network/internet access rights
- Warning
- Further sanction e.g. detention/exclusion

## Appendix 1

### School Technical Security Policy

#### Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the *school infrastructure/network* is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems
- there is oversight from senior leaders and these have impact on policy and practice.

#### Responsibilities

The management of technical security will be the responsibility of the school's computing technician.

#### Technical Security

##### Policy statements

The school will be responsible for ensuring that their infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people receive guidance and training and will be effective in carrying out their responsibilities:

- school/academy 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 must be securely located and physical access restricted
- appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data
- responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff
- all users will have clearly defined access rights to school technical systems. Details of the access rights available to groups of users will be recorded by the network manager/technical staff/other person and will be reviewed, at least annually, by the online safety group.
- users will be made 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

- The computing technician is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- mobile device security and management procedures are in place
- school/local authority/managed service provider/technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.
- remote management tools are used by staff to control workstations and view users activity
- an appropriate system is in place for users to report any actual/potential technical incident to the online safety co-ordinator/network manager/technician (or other relevant person, as agreed)
- visitors to the school may be offered temporary access to the school's guest network (unifi-guest).
- the downloading of executable files and the installation of programmes on school devices will be carried out by the school's computer technician
- the school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc.
- personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

### **Password Security**

A safe and secure username/password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and learning platform). You can find out more about passwords, why they are important and how to manage them in our blog article. You may wish to share this with staff members to help explain the significance of passwords as this is helpful in explaining why they are necessary and important.

### **Policy Statements:**

- These statements apply to all users.
- All school networks and systems will be protected by secure passwords.
- All users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the online safety group (or other group).
- All users (adults and students/pupils) have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Passwords must not be shared with anyone.
- All users will be provided with a username and password by the computer technician who will keep an up -to-date record of users and their usernames.

### **Password requirements:**

- Passwords should be long. Good practice highlights that passwords over 12 characters in length are considerably more difficult to compromise than shorter passwords. Passwords generated by using a combination of unconnected words that are over 16 characters long are extremely difficult to crack. Password length trumps any other special requirements such as uppercase/lowercase letters, number and special characters. Passwords should be easy to remember, but difficult to guess or crack.

- Passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school
- Passwords must not include names or any other personal information about the user that might be known by others
- Passwords must be changed on first login to the system
- *The school may wish to recommend to staff and students/pupils (depending on age) that they make use of a 'password vault' these can store passwords in an encrypted manner and can generate very difficult to crack passwords. There may be a charge for these services.*
- *Passwords should not be set to expire as long as they comply with the above, but should be unique to each service the user logs into.*

### **Training/Awareness:**

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

- at induction
- through the school's online safety policy
- through the acceptable use agreement

Students/pupils will be made aware of the school's/college's password policy:

- in lessons
- through the acceptable use agreement

### **Audit/Monitoring/Reporting/Review:**

The Online Safety Lead will ensure that full records are kept of:

- User Ids and requests for password changes
- User logons
- Security incidents related to this policy

## Appendix 2

## Reporting Log

Group: .....

[illegible]

## Appendix 3

### Pupil Acceptable Use Policy Agreement

#### ***This is how we stay safe when we use computers:***

- I will ask a teacher or suitable adult if I want to use the computers/tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of computers/tablets and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer/tablet

Signed (child): .....

## Appendix 3

### Staff (and Volunteer) Acceptable Use Policy Agreement

#### **School Policy**

New technologies have become integral to the lives of children and young people in today's society, both within schools/academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

#### **This acceptable use policy is intended to ensure:**

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school/academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for *students/pupils* learning and will, in return, expect staff and volunteers to agree to be responsible users.

#### **Acceptable Use Policy Agreement**

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students/pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the *school/academy* will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the guidelines set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using *school* systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with students/pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the *school*

- When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using *school/academy* equipment. I will also follow any additional rules set by the *school/academy* about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school/academy policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the school policy). Where digital personal data is

transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.

- I understand that data protection policy requires that any staff or student/pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school/academy policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

**When using the internet in my professional capacity or for school sanctioned personal use:**

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that I am responsible for my actions in and out of the *school*.
- I understand that this acceptable use policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school/academy systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school/academy
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors/directors and/or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name: .....

Signed: .....

Date: