Mill View
Online Safety Policy
2024-2025

Contents

Development / Monitoring / Review of this Policy

This Online Safety policy has been developed by a working group made up of:

- Headteacher/Deputy Headteacher
- Computing Leads / Online Safety Lead
- Staff – including Teachers, Support Staff, Technical staff
- Governors / Board
- Parents and Carers

Consultation with the whole academy community has taken place through a range of formal and informal meetings in its original development.

Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the Board of Directors / Governing Body / Governors Sub Committee on:	Date:
The implementation of this Online Safety policy will be monitored by the:	Headteacher, Deputy Head Online Safety Lead, Computing Leads
Monitoring will take place at regular intervals:	At least once per annum
The Board of Directors / Governing Body will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	Once per annum
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	Next review date: Spring 2026
Should serious online safety incidents take place, the following external persons / agencies should be informed:	Steve Ellis – CEO, CAT Luci Jones – Director of Operations, CAT Police (if required) Local Safeguarding Teams (if required)

Mill View Primary School will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering • Internal monitoring data for network activity
- Surveys & questionnaires
- Audit activity as required throughout the year to prevent, as well as in response to any online safety incidents arising.

Scope of this policy

This policy applies to all members of Mill View Primary School (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of **any** academy digital technology systems, both in and out of the academy. It is paramount to ensuring that children and staff are well protected against dangers in relation to online safety, and that robust systems are in place which will enable children and staff to use technology for the benefit of outstanding teaching and learning, safely and in line with best practice and relevant legislation.

The Education and Inspections Act 2006 empowers the Headteacher to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the academy 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 academy, but is linked to membership of the academy. 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 academy 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.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within Mill View Primary 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 in line with their role as Safeguarding Governor. The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Coordinator / Officer
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- updates and reporting to relevant Governors / Board / Committee / meetings.

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Officer / 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. This process can be found in flow chart form in appendix 6.
- The Headteacher and Senior Leaders are responsible for ensuring that the Online Safety Officer / 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 ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles. These systems will include:
  - Up to date acceptable usage statements for all pupils within Mill View Primary,

- Up to date acceptable usage statements for all staff and volunteers within Mill View Primary, ○ Central records of reports of misuse of technology within Mill View Primary, including reports, investigations and outcomes,
- Central records of monitoring logs of online safety incidents and appropriate action(s) arising from such incidents.
- Central records of staff training and INSET given in relation to matters of Online Safety.

- The Senior Leadership Team / Senior Management Team will receive regular monitoring reports from the Online Safety Officer.

Online Safety Officer – Harry Morris / Computing Leads - Emma Hutcheson and Harry Morris

- leads the Online Safety Group
- 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 / MAT / relevant body
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety development
- meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors / Directors
- reports regularly to Senior Leadership Team

Network Manager / Technical staff- Dan Wooley

Mill View receives technical support through a formal service level agreement with D Wooley. They are responsible for ensuring:

- that the academy's technical infrastructure is secure and is not open to misuse or malicious attack
- that the academy meets required online safety technical requirements and any Local Authority / MAT / other relevant body Online Safety Policy / Guidance that may apply,
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed,
- 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 network / internet / Learning Platform / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / Senior Leaders; Online Safety Officer / Lead for investigation / action / sanction,
- that monitoring software / systems are implemented and updated as agreed in academy 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 academy Online Safety Policy and practices,
- they have read and understood the Staff Acceptable Use Policy / Statement (AUP) (See appendix 1)
- they report any suspected misuse or problem to the Headteacher / Senior Leader; Online Safety Officer for investigation / action / sanction,
- 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,
- students / pupils understand and follow the Online Safety Policy and acceptable use policies,
- 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 students / 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 Ali Gibbons (DDSL Katie Hetherington/Joy Nicholls)

Will 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 online contact with adults / strangers
- potential or actual incidents of grooming
- online-bullying

Students / Pupils:

- are responsible for using the academy digital technology systems in accordance with the Student / Pupil Acceptable Use Statement (see appendix 2/3)
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations (where applicable)
- 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 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.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The academy will take every opportunity to help parents understand these issues through parents’ evenings, newsletters, letters, website / Learning Platforms and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the academy 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 academy (where this is allowed)

Community Users

Where applicable, Community Users who access academy systems / website / Learning Platform as part of the wider academy provision will be expected read the Community User AUA before being provided with access to academy systems.

Policy Statement - Education

The following statements document how Mill View educates all academy stakeholders in relation to matters of online safety.

Protecting Children Online: The 4C’s of Online Safety

Requirement of Keeping Children Safe in Education (KCSiE) 2024
In line with the statutory guidance outlined in KCSiE 2024, Bexton Primary School recognises the importance of educating pupils to navigate the online world safely and responsibly. A core component of this guidance involves equipping children with an understanding of the 4C’s of online safety: **Content, Contact, Conduct, and Commerce.** These categories represent key areas of risk in the digital landscape and form the foundation for our online safety education.

Understanding the 4C’s of Online Safety

- **Content**: Risks related to exposure to harmful or inappropriate material, including violent, extremist, or sexually explicit content, as well as misinformation.
- **Contact**: Risks of harmful interactions with others online, such as cyberbullying, grooming, or contact with strangers.
- **Conduct**: Risks stemming from a child’s own behaviour, including sharing personal information, engaging in cyberbullying, or other activities that compromise their or others’ safety.
- **Commerce**: Risks associated with online transactions, such as scams, phishing, and exploitative financial practices aimed at children.

Our Approach to Embedding the 4C’s in the Curriculum
To ensure comprehensive coverage of the 4C’s, Bexton Primary School uses the following educational resources:

Kapow Computing Curriculum: This scheme of work includes structured online safety lessons delivered each half term, addressing all aspects of the 4C’s in an age-appropriate manner.

An overview of the curriculum coverage for Computing and PSHE, including specific references to online safety, can be found on the school website.

By combining these resources and adhering to the guidance in KCSiE 2024, Bexton Primary School aims to empower children to navigate the digital world safely, fostering resilience and critical thinking in online environments.

Educating 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 academy's online safety provision. Children need the help and support of the academy 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 / RHSE / other lessonsand should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- 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 Statement (see appendix 2/3) and encouraged to adopt safe and responsible use both within and outside the academy.
- Pupils should be made aware of the legal age of using social networking sites, and legal ramifications for things posted online, alongside other dangers they pose.
- 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 students / 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 (eg 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 recorded by the Online Safety lead, with clear reasons for the need.

Educating parents and carers

Many parents and carers have only a limited understanding of online safety risks and issues, particularly within the ever changing technological age we find ourselves in. However, they play an essential role in the education of their children and in the monitoring / regulation of their 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.

Mill View Primary 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 relevant web sites, publications and support materials.

Educating and training staff, governors and 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:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly, with central records of training being held on staff files.
- All new staff will receive online safety training from the Online Safety Lead as part of their induction programme, ensuring that they fully understand the academy Online Safety Policy and Acceptable Use Statement.
- In the event any staff identify online safety as a training need within the performance management process, appropriate training and support will be given to such staff members as required through the Online Safety Lead or relevant external providers.
- The Online Safety Lead (or other nominated person) will receive regular updates through attendance at external training events.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Online Safety Lead (or other nominated person) will provide advice / guidance / training to individuals as required.

Policy Statement – Safer Use of Technology in Mill View

Mill View uses a wide range of technology. This includes access to: •
Computers, laptops and other digital devices

- Ipads
- Internet which may include search engines and educational websites
- Learning platform/intranet
- Email
- Game and interactive based technologies
- Digital cameras, web cams and video cameras

All setting owned devices will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place.

- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- We will ensure that the use of internet-derived materials, by staff and learners complies with copyright law and acknowledge the source of information.
- Supervision of learners will be appropriate to their age and ability.

Early Years Foundation Stage and Key Stage 1

- Access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the learners age and ability.

Key Stage 2

- Learners will use age-appropriate search engines and online tools.
- Learners will be directed by the teacher to online materials and resources which support the learning outcomes planned for the learners age and ability.

Managing Access to the Internet

All staff, learners and visitors will read and understand an acceptable use policy before being given access to our computer system, IT resources or internet. Examples of these can be found in this policy's appendices.

Policy Statement – Technical – infrastructure, filtering and monitoring

Mill View will be responsible for ensuring that the academy 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 ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities. Whilst the academy has an overall responsibility to ensure the following criteria are met, it will work with D. Wooley to ensure:

- Academy technical systems will be managed in ways that ensure that the academy meets recommended technical requirements,
- There will be regular reviews and audits of the safety and security of academy technical systems, • Servers, wireless systems and cabling must be securely located and physical access restricted,
- All users will have clearly defined access rights to academy technical systems and devices.
- All users (at KS2 and above) will be provided with a username and secure password by the academy who will keep an up to date record of users and their usernames.
- The "master / administrator" passwords for the academy ICT 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 (eg academy safe).
- Office staff 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.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. Where changes to filters are requested, they are logged and kept on central record with reasons why the change was requested and the merit it held.
- Internet filtering / monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- Academy technical staff regularly monitor and record the activity of users on the academy technical systems and users are made aware of this in the Acceptable Use Statements (see Appendices).
- An appropriate system is in place (by reporting to the Online Safety Lead) for users to report any actual / potential technical incident / security breach to the relevant person, which is then recorded on the reporting pro forma (see appendix 4).
- 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 workstations are protected by up to date virus software.

- In the event that any personal device is allowed to be connected to the academy network, users abide by the acceptable usage policy and the terms detailed within it.

Policy Statement – Mobile devices

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational and must abide by the acceptable usage statements when using any mobile device. The regulation of mobile devices within Mill View is shown in the following diagram.

	School Devices			Personal Devices		
	School owned for single user	**School owned for multiple users**	**Authorised device**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	Yes	Yes	Yes	At discretion of Headteacher[1]	Yes	Turned off/placed away except where needed for purpose of visit – then after reading AUA.
Full network access	Yes	Yes	Yes	None	After readin g AUA	As above, and only if required for the intended purpose of their visit (i.e. contractors).

[1] There may be occasions where the Headteacher feels it is a requirement that a student owned or visitor owned mobile device is allowed onto the premises, such as in relation to a safeguarding incident or investigation, or as is required on medical grounds. These instances are to be determined by the Headteacher and are allowed under their discretion.

Staff Use of Personal Devices and Mobile Phones

Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant policy and procedures, such as: confidentiality, child protection, data security and acceptable use.

Staff will be advised to:

- Keep mobile phones and personal devices in a safe and secure place (e.g. in a private locker/drawer) during lesson time.
- Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
- Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.
- Not use personal devices during teaching periods, unless written permission has been given by the Headteacher, such as in emergency circumstances.
- Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.

Members of staff are not permitted to use their own personal phones or devices for contacting learners or parents and carers.

- Any pre-existing relationships, which could undermine this, will be discussed with the DSL (or deputy) and/or Headteacher.

Staff will not use personal devices:

- To take photos or videos of learners and will only use work-provided equipment for this purpose.
- Directly with learners and will only use work-provided equipment during lessons/educational activities.
- If a member of staff breaches our policy, action will be taken in line with our code of conduct/staff behaviour and allegations policy

If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.

Visitors' Use of Personal Devices and Mobile Phones

Parents/carers and visitors (including volunteers and contractors) should ensure that they have read the safeguarding notice upon entering the academy building, and that they do not use their personal devices until they have left the premises, unless required to do so in order to complete the purpose of their visit. They are encouraged to leave such devices with the office for safekeeping for the duration of their visit, or asked to place it away in a safe and secure place, and abide by the acceptable use statements form prior to entering the building.

We will ensure appropriate signage and information is displayed and provided to inform parents, carers and visitors of expectations of use.

Visitors (including volunteers and contractors) who are on site for a regular or extended period will use their mobile phones and personal devices in accordance with our acceptable use policy and other associated policies, such as: anti-bullying, behaviour, child protection and image use.

Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL (or deputy) of any breaches our policy.

Policy Statement – The 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 students / pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying 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 academy will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students / 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 students / 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 (but not other) children at academy events for their own personal use (as such use in 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. If an event involves multiple children, and it is not possible for the parent / carer to individually photograph/video their child without capturing other children, they will not be permitted to take photographs/videos.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on academy equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the academy into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include students / 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.

Policy Statement - Data Protection

With effect from 25th May 2018, the data protection arrangements for the UK changed following the European Union General Data Protection Regulation (GDPR) announced in 2016. How Mill View Primary conforms to the updated requirements of the above legislation, as well as how this supports this Online SafetyPolicy can be found within the academy's Data Protection Policy. However certain aspects of Online Safety cross over into data safety also, as detailed in the next section.

Policy Statement – Data Security

The academy will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

The academy will ensure that systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

All users will use strong passwords which must be changed regularly. User passwords must never be shared.

Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data can only be stored on school equipment (this includes computers and portable storage media (where allowed). Private equipment (i.e. owned by the users) must not be used for the storage of personal data.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected,
- the device must be password protected,
- the device must offer approved virus and malware checking software and,
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Even if the above criteria is satisfied, the preferred method of accessing and sharing data types will be using the cloud based system, OneDrive, or Teams, which offers encrypted services as standard. All school users have their own OneDrive/Teams account and must not share usernames, or passwords. Where sharing and collaboration on documents does occur, this should be done via the OneDrive/Teams app sharing facility, thus ensuring continuity in the data integrity.

Secure transfer of data and access out of school

The academy recognises that personal data may be accessed by users out of school, or transferred to other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location.
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (eg family members) out of school
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location;
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software.

Policy Statement – Communication

Communication is of paramount importance to furthering children's education. As such, the communication from staff to home is actively encouraged, however in order to promote the highest standards of online safety, to comply with data protection and child safeguarding legislation, as well as to keep staff and the academy itself protected, this communication has to take place within the appropriate parameters as set out in detail below.

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

- The official academy email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff should therefore use only the academy email service to communicate with others when in school, or on academy systems (e.g. by remote access).
- Users must immediately report, to the nominated person (Headteacher, Vice Headteacher or Online Safety Lead), 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 students / pupils or parents / carers (email, social media, chat, blogs, VLE, pings etc) must be professional in tone and content. These communications may only take place on official (monitored) academy systems. Personal email addresses, text messaging or social media must not be used for these communications in any circumstance.
- 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. These lessons will be taught through designated Online Safety lessons, RSHE lessons, assemblies and external visits from Online Safety Professionals.
- Personal information should not be posted on the academy website and only official email addresses should be used to identify members of staff.
- When emailing sensitive information which may breach data protection regulations Egress Switch will be used to send the information securely.

Policy Statement - Social Media Use – Protecting Professional Identity

The increase in popularity of social media, along with its ever increasing presence within society in ever changing forms has huge potential ramifications for online safety of the children, parents / carers and staff associated with Mill View Primary. All schools, academies, MATs and local authorities have a duty of care to provide a safe learning and working 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 academy or local authority / MAT liable to the injured party.

Mill View provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published,
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues,
- Clear reporting guidance, including responsibilities, procedures and sanctions,
- Risk assessment, including legal risk.

With this in mind, academy staff should ensure:

- No reference should be made in social media to students / pupils, parents / carers or academy staff,
- They do not engage in online discussion on personal matters relating to members of the academy community,
- Personal opinions should not be attributed to the academy or local authority / MAT,
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information,
- They are not 'connected' on any social media platform to present or past pupils, or parents (except where a prior friendship or relationship exists).
- They do not make or include themselves by commenting, liking or sharing posts which could be deemed offensive or inflammatory in relation to areas such as religion, race, sex, politics, personal beliefs etc. (including the posting of memes and graphics).
- Personal accounts do not interact with any school social media accounts, thus crossing the professional boundaries set out in the acceptable usage statement.

As part of its outreach and continued engagement with the wider community, Mill View Primary itself has a social media presence. The above rules apply to these accounts, and best practise will be ensured by the following monitoring activities:

- The academy's use of social media for professional purposes will be checked regularly by the Online Safety Lead to ensure compliance with academy policies,
- Communication will be one way, and accounts will be locked to prevent open dialogue occurring via any Social Media portal.
- Followers, comments, likes and other forms of interaction will be vetted by the person(s) in charge of the accounts.
- The academy's use of social media for professional purposes will be checked regularly by the Online Safety Lead to ensure compliance with academy policies,
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff, namely the Headteacher and Online Safety Lead.
- Systems for reporting and dealing with abuse and misuse.

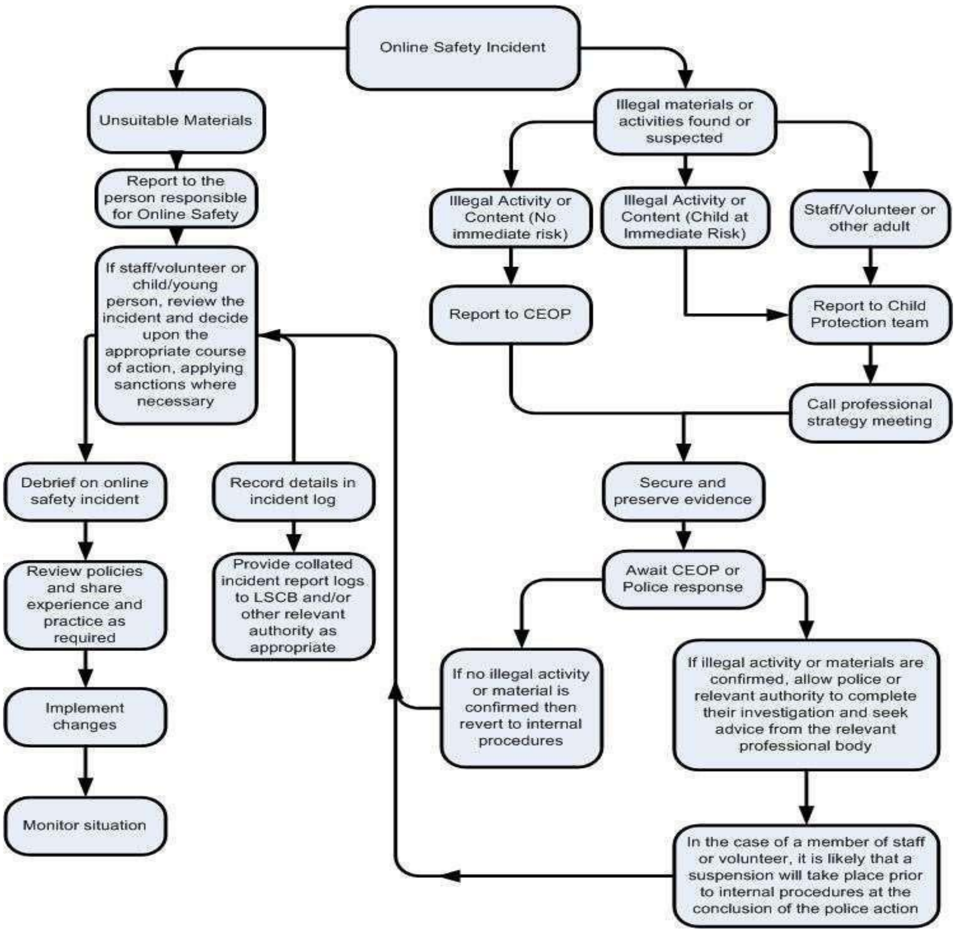
Policy Statement - Dealing with unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from academy 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 an academy context, either because of the age of the users or the nature of those activities.

Mill View believes that the activities referred to in the acceptable usage statements for staff would be inappropriate in an academy context and that users should not engage in these activities in / or outside the academy when using academy equipment or systems.

Policy Statement – Reporting and Responding to Online Safety Incidents

This guidance is intended for use when staff need to report / 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, however may arise out of mistakes made by individuals when using connected devices or otherwise well intentioned users. If there is any suspicion that the web site(s) / platform concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right Flowchart (below and appendix 6) for responding to online safety incidents and report immediately to the police



Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

It is hoped that all members of the academy community will be responsible users of digital technologies, who understand and follow academy 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 should 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 Local Authority / Academy Group or national / local organisation (as relevant). • 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 o other criminal conduct activity or materials

Those staff members involved in the process of reporting the incident(s) should isolate the computer in question as best they 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 academy 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.

Where other incidents may occur in relation to an Online Safety threat which is not linked to something which has happened on the academy system, staff should escalate it in accordance with the safeguarding policy, treating it as a safeguarding incident.

Policy statement - Academy sanctions

It is more likely that the academy 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. Any incidents of deliberate misuse of technology, in breach of any part of this Online Safety Policy will be dealt with in accordance with academy's disciplinary policy.

Appendix 1 Staff and Volunteer Acceptable Use Statement

Staff (and Volunteer) Acceptable Use 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 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 pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Statement:

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 academy will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this statement also apply to use of these technologies (e.g. laptops, Ipads, email, 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 policies and rules 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 (DSL, DDSL, Online Safety Officer).

I will be professional in my communications and actions when using academy ICT 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

(eg on the school website, Twitter) 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. Facebook and Twitter accounts are linked and therefore anybody who adds information, including pictures and opinions, are held solely liable for those and must act sensibly and with thought in line with maintaining the school's community reputation.
- 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 Academy and the Local Authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the academy:

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc) in school, I will follow the rules set out in this statement, in the same way as if I was using academy equipment. I will also follow any additional rules set by the 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 academy 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 academy policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist 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, unless this is allowed in academy policies.
- I will not disable or cause any damage to academy 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 Academy / LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted 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 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 academy:

- I understand that this Acceptable Use Policy applies not only to my work and use of academy digital technology equipment in school, but also applies to my use of 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 academy
- I understand that if I fail to comply with this Acceptable Use Policy Statement, I could be subject to disciplinary action. This could include a verbal or formal warning, a suspension, referral to Directors 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.

Appendix 2 KS1 Pupil Acceptable Use Statement

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 the computer and other equipment,
- I will not speak to other people online without an adult present,
- 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,

Appendix 3 KS2 Pupil Acceptable Use Statement

Academy Policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These 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. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Statement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use,
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the students / pupils to agree to be responsible users.

Acceptable Use Policy Statement

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.

For my own personal safety:

- I understand that the academy will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, 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 be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the academy systems and devices are intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not use the academy systems or devices for on-line gaming, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the academy:

- I will only use my own personal devices (mobile phones / USB devices etc) in school if I have permission.

- I understand that, if I do use my own devices in the academy, I will follow the rules set out in this statement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I 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 immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, 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 not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.

When using the internet for research or recreation, I recognise that:

- I should 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 try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the academy also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this statement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Statement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, contact with parents and in the event of illegal activities involvement of the police.

Student / Pupil Acceptable Use Statement Form

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Statement.

I have read and understood the above and agree to follow these guidelines when:

- I use the academy systems and devices (both in and out of school)
- I use my own devices in the academy (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I use my own equipment out of the academy in a way that is related to me being a member of this academy e.g. communicating with other members of the school, accessing school email, website etc.

Appendix 4 Reporting log of online safety incident

Reporting Log

Group:

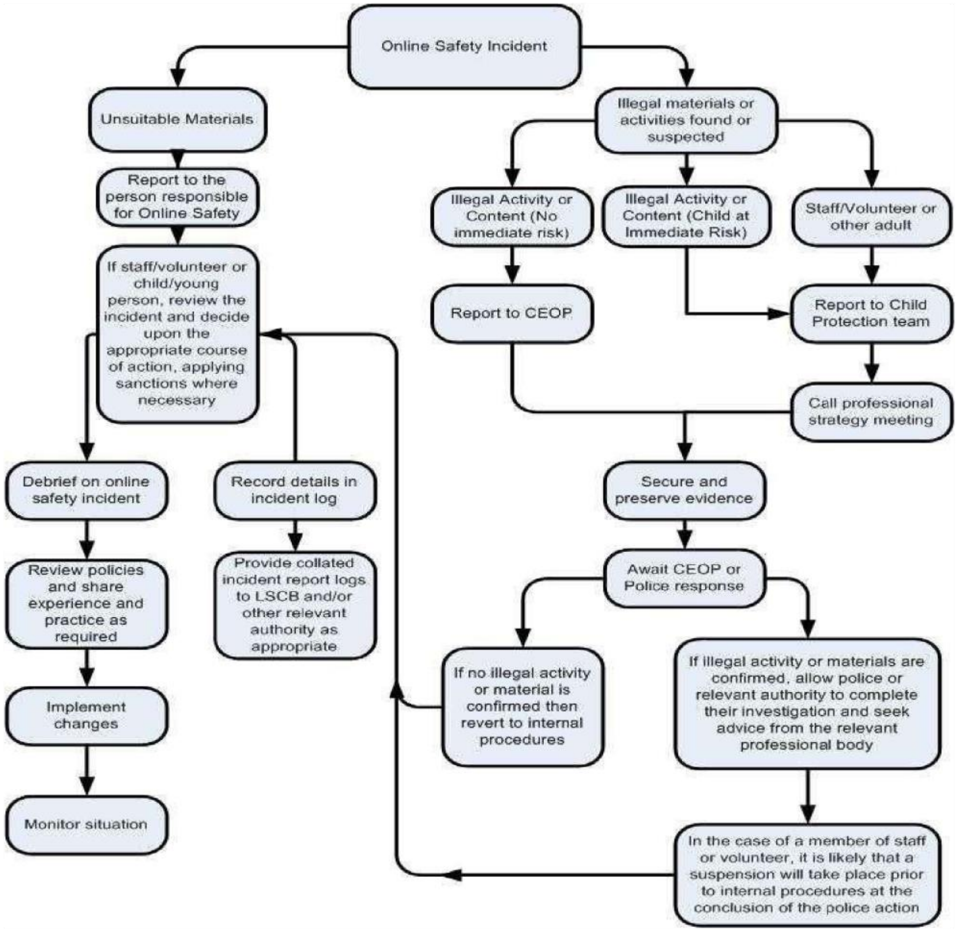
Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		

Appendix 5 Online Safety staff training log

Training Log: Online Safety Group:

Staff member	Training given and date	Trained by	Cost	Review Date

Appendix 6 Reporting and Responding to Online Safety Incident



Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action