MILLWOOD SCHOOL, BURY

POLICY: Online Safety Policy (formerly E-Safety Policy)

DATE: April 2014

Date Reviewed: May 2016 (CH)

DATE ADOPTED BY GOVERNING BODY: ……

Introduction

Millwood Primary Special School recognises the importance of ICT in education and the need of pupils to access the computing facilities available within the School. The School aims to make the ICT facilities it has available for pupils to use for their education but realises that this has to be controlled for their safety.

Safeguarding children in both the real and virtual world is everyone's responsibility. Computers and technology can be a great way to open up new learning opportunities to our children but it also means we have to be aware of the possible risks. E-safety encompasses the use of Internet technologies, electronic communications and wireless technology.

This policy provides a framework for us to ensure ICT is used safely and responsibly and that risks related to ICT use is properly managed. At Millwood the safety of our pupils is our first priority. We ensure that all staff are aware of their responsibilities and have clear policies and procedures that must be followed. This is supported by effective technological tools that protect the aspects of the internet that the children can access.

Millwood School subscribes to the BOOST+ Online Safety Toolkit to support us with professional development and to manage online safety.

Keeping Children Safe in Education (2106) states that,

"The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation, radicalisation, sexual predation: technology often provides the platform that facilitates harm."

"The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- Content: being exposed to illegal, inappropriate or harmful material;
- Contact: being subjected to harmful online interaction with other users:
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm." (KCSIE 2016)

It is the duty of the school to ensure that every child is safe, and the same principles should apply to the digital world as would be applied to the school's physical building.

Technical – infrastructure / equipment, filtering and monitoring
Millwood School ensures that the infrastructure and network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented and that people named in this policy by name or role are effective in carrying out their online safety responsibilities.

We employ PC Edutech to manage the technical systems in ways that ensure we meet recommended technical requirements. This includes scheduled "health checks" on the network, workstations and servers and make recommendations on work required when necessary. The contract also includes managed updates of Operating Systems, Managed updates on anti-virus software, Internet Connectivity and performance management, Network user management, Network fault finding and troubleshooting as well as advice, support and set up of a range of hardware and software to aid teaching and learning.

Servers, wireless systems and cabling are securely located and kept locked.

The IT technician, from PC Edutech manages the access rights to systems and devices, including holding and managing passwords where appropriate. The "master / administrator" passwords for the school / academy ICT system, used by the IT technician are available to PC Edutech and the Headteacher and stored on a secure document held by PC Edutech and available to the Headteacher on request

The IT technician is responsible for ensuring that software licence logs are accurate, up to day and that regular checks are made to reconcile the number of licences purchased against the number of software installations

The IT technician ensures that appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.

The IT technician manages the provision of temporary access of guests onto the school systems.

- Visitors may log onto the system using the visitor log in. The visitor log in gives access to the internet and and programs installed on the computer. Requests to use the wifi will be considered on an individual basis and the code can only be entered by the IT technician or member of the SMT.
- Supply teachers on a long term placement use class log ins to access the same areas as class teachers. They may be given an school email account and log ins to the assessment and tracking tool used by the IT Technician. Once the placement is finished the IT technician will block the email account and remove the log ins. Supply staff are given the Acceptable Use Policy on arrival and are expected to follow the policy and procedures. If we have any concerns about their online use this will be raised with their employers, usually Teaching Personnel, and the LADO if appropriate. The Headteacher will ensure the employer completes an investigation.

All staff with access to IT equipment sign an Acceptable Use agreement in September each year and additionally on receipt of any new mobile devices. This agreement states:

- School devises must only be accessed by school staff and used for professional purposes.
- Data must not be stored on USB storage devices that are not encrypted and password protected. School will provided secure USB storage devices to staff who need to take school information off site. No school information may taken off site unless it is encrypted and password protected.
- Only the IT technician can install programs on school based computers. SMT, Teachers and HLTAs may install free apps on mobile devices in order to test the suitability for school use.
- If any device completes an auto update this must be reported to the IT technician and the mobile device returned to him in order to have the settings rechecked.

Millwood Primary Special School provides internet filtering, designed to remove controversial, offensive or illegal material that would cause our children to be upset or vulnerable to abuse, for all users. Illegal content (child sexual abuse images) is filtered by the filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. Internet filtering ensures that children are safe from terrorist and extremist material when accessing the internet, in line with the additional duties for schools under the Counter Terrorism and Securities Act 2015. The School makes use of the filtering services provided by the Local Authority which seeks to provide internet use that is safe and for educational purposes only. The Local Authority provide filtering and monitoring services from Fortinet who have completed the provider checklist response published by the UK Safer Internet Centre as highlighted in KCSIE. (Please see attachments at end of this policy)

We ensure that all staff are aware that no filtering system is fool proof and additional measures need to be taken to minimise the risks:

- ***All access to the Internet is supervised by adults****.*

- Safe Search is used on all pupil computers to enhance filtering.

- Safe internet use is included in the formal ICT curriculum for any pupil working at level P8 or above or earlier if the pupil is able to access the internet independently.

- Any search engine or keyword search you ask a child to do must have been tested in advance on that day to ensure the child will not encounter anything that could be upsetting.

Use of electronic equipment including mobile technologies

- The school allows the following use of mobile technologies

	School Devices			Personal Devices		
	School owned for single user	School owned for multiple users	Authorised device (eg CYPIC)	Student owned	Staff owned	Visitor owned
Allowed in school	*Yes*	*Yes*	*Yes*	*No*	*Yes*	*Yes*
Full network access	*Yes*	*Yes*	*Yes*	*No*	*No*	*No*
Internet only				*No*	*No*	*No – unless by prior agreement and managed by IT technician*
No network access				*No*	*No*	*No*

School owned devices are provided to members of the SMT, Class Teachers, HLTAs, Office Manager and Duty officer from Premises Team. The use of these devices are outlined on the Acceptable use policy which is signed by all staff allocated devices. The IT technician is responsible for managing these devices. The devices are subject to the Local Authority filtering system. When the member of staff leaves the school the devices are returned to the IT technician who blocks the email and clears the device. Training is provided by IT technician when the device is allocated and the CPD coordinator will organise further training where necessary.

Laptops and other school equipment should be used appropriately at all times and staff, workers and volunteers should ensure that usage does not conflict with their role or professional duties. (See ICT –Acceptable use policy).

School owned laptops and iPads are insured by the school for use off site.

Where personal data is stored on any portable computer system, memory stick or any other removable media the data must be encrypted and password protected, the device must be password protected, have approved virus and malware checking software and be deleted from the device once it has been transferred or its use is complete

Staff must never use their own equipment for taking photographs or video of pupils.

Only school SIM cards and equipment should be used and images stored on the shared drive which is secure and managed by the ICT technician who is DBS-checked.

Personal devices may be used as outlined in the above table. Signs are displayed in the School Reception informing visitors that they may not use mobile phones in areas accessed by children during school hours.

Pupils are not permitted to bring mobile devices to school.

Staff may only use personal devices such as mobile phones during non-class time, such as breaks and after pupils have gone home. When pupils are on site mobile phones must be switched off in classrooms and areas when pupils are present and only used in areas of the school where pupils are not permitted such as the staff room, staff prep room and office areas. Mobile phones should be stored in areas locked from pupil access.

Staff may use their personal devices for school business such as sending an email or texting a professional but must ensure they do not share their phone number with a pupil or their family.

Staff are not able to access the school network or wifi on their personal device.

There is no technical support available for personal devices.

Staff will have due regard to the data protection policy when using their personal devices.

Staff must not take any image in school on their personal devices.

The school will not be liable for any loss, damage or malfunction following any use of personal devices in school.

Education about the safe and responsible use of mobile devices is included in the school Online Safety education programmes – see E-Safety scheme of work

Data Protection

Personal data is recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

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

See Data Protection Policy for further details

Communication with pupils

Any private communication with an individual pupil or their family should be recorded and copied to the pupil's file, with the exception of the home school diary.

Any digital communication between staff and pupils or parents / carers 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.

Personal telephone numbers, including mobile numbers should not be shared with pupils or families, other than in emergency situations. If a pupil continues to use these personal contacts, this should be reported immediately to the designated teacher for safeguarding.

Improper communication between staff, workers and volunteers and a pupil is likely to result in disciplinary action.

No e-mail communication should occur which does not pass through the school network mails boxes and addresses.

Staff, workers and volunteers should not participate in chat rooms, MSN or social networking sites with any pupils irrespective of age or with former pupils under the age of 18. In particular, staff, workers and volunteers should neither accept nor request pupils or former pupils under the age of 18 as friends on Facebook or other social networking sites. Staff, workers and volunteers should be mindful of the impact on younger siblings or friends of former pupils in any social contact.

No text conversation should take place between staff, workers and volunteers and a pupil. In the event of this happening it should be recorded and placed on the pupil's file, and reported to the Headteacher – Helen Chadwick, or in her absence the designated safeguarding lead – Caroline Henley

Staff, workers and volunteers using social networking sites in a personal capacity should ensure that they do not conduct themselves in a way that is detrimental to the school. For example they should not:

- allow interaction on websites to damage or compromise working relationships with colleagues.
- allow interaction on websites that damage or compromise the good name of the school
- enter into electronic conversations relating to the school or its pupils with any family members of pupils
- post photographs of themselves, colleagues or students taken in school
- post or send abusive or defamatory messages
- record any confidential information about school on any social networking site
- post information which will disclose the identity of a student.

Communications

The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).

Users must immediately report, to the SMT 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. At Millwood we use the Online Safety BOOST+ system that includes an anonymous reporting app Whisper

Whole class email addresses may be used with pupils

Pupils will be taught about online safety issues, such as the risks attached to the sharing of personal details. They will also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

Personal information must not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media
All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party.

Millwood School has a school website that is updated by the Headteacher and IT technician. This is the only social media account held and run by the school.

Personal Use 0f Social Media
Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy

Personal communications which do not refer to or impact upon the school are outside the scope of this policy

Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

Monitoring of Public Social Media
As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school

Millwood uses the Online Safety BOOST+ system that includes Reputation Alerts that highlight any reference to the school/academy in online media.

Use of video equipment

In pupil performances, for example, Christmas productions, parents and carers may take video or photographs of their own child. They must sign a disclaimer form available at each performance to say they will film or photograph their own child only, and that they take responsibility for storing the image of their child safely, not sharing it on social networking sites.

More explicit information is available in the Millwood School Photography Guidance from Bury MBC (2015)

Curriculum

A planned online safety curriculum is provided as part of the Computing, PHSE and cross curricular lessons involving any form of ICT – see scheme of work on shared area. This is based on the use of selected kidsmart, thinkuknow and childnet materials

Key online safety messages are reinforced as part of a planned programme of assemblies nurture group and class activities

Where appropriate to the pupil's cognitive development, pupils will be taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information.

Where appropriate to the pupil's cognitive development, pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

Where appropriate to the pupil's cognitive development, pupils will be supported to build resilience to radicalisation by providing a safe environment for discussion and helping them to understand how they can influence and participate in decision making in line with the duty for schools to ensure that children are safe from terrorist and extremist material on the internet

Where appropriate to the pupil's cognitive development, pupils are 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 act as good role models in their use of digital technologies the internet and mobile devices

In lessons where internet use is pre-planned, pupils will be guided to sites checked as suitable for their use.

In the event that any unsuitable material is found this is immediately reported to the ICT technician and to the SMT and the device will be closed down until cleared by the ICT technician.

Where students / pupils are allowed to freely search the internet, staff must be vigilant in monitoring the content of the websites the young people visit with **no child allowed unsupervised access to the internet at any time**.

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 ICT technician temporarily remove those sites from the filtered list for the period of study. Any request to do so must be agreed by a member of the SMT in writing prior to the request.

PARENTS

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 on-line 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
- Parent coffee mornings
- High profile events / campaigns e.g. Safer Internet Day
- Membership of Digital schools displayed on the website enabling parents free access to parentzone program

CCTV

The school's use of CCTV is restricted to Premises managers and the SMT. Footage is stored for 30 days, after which it is overwritten by new footage. All accommodation outside the school on School Street has been 'blocked'.

No visitor to the school site is allowed to take photographs or video without the permission of the school management team and any parent or carer who has responsibility for a child. Any breaches of this policy will be referred to the LADO for Bury, and reported to OFSTED.

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 / academy policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	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	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal					X	

information, databases, computer / network access codes and passwords)					
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				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	X		
Use of video broadcasting e.g. Youtube		X	X		

Reporting Problems

An important element of e-safeguarding is the ability to identify and deal with incidents so they are dealt with effectively. If there is ever an issue, concern or incident related to e-safety it should be recorded on the safety incident form attached and handed directly to the designated teacher for safeguarding, who will follow the appropriate procedures (outlined in the attached flowchart).

Complaints of cyberbullying are dealt with in accordance with our school Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school/ LA child protection procedure.

This policy has been drawn up to protect all parties- the pupils, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

At Millwood we use the Online Safety Boost+ tool to help pupils to report problems with a single click. Where appropriate to the pupil's cognitive development, pupils are taught to recognise when and how to report their concerns.

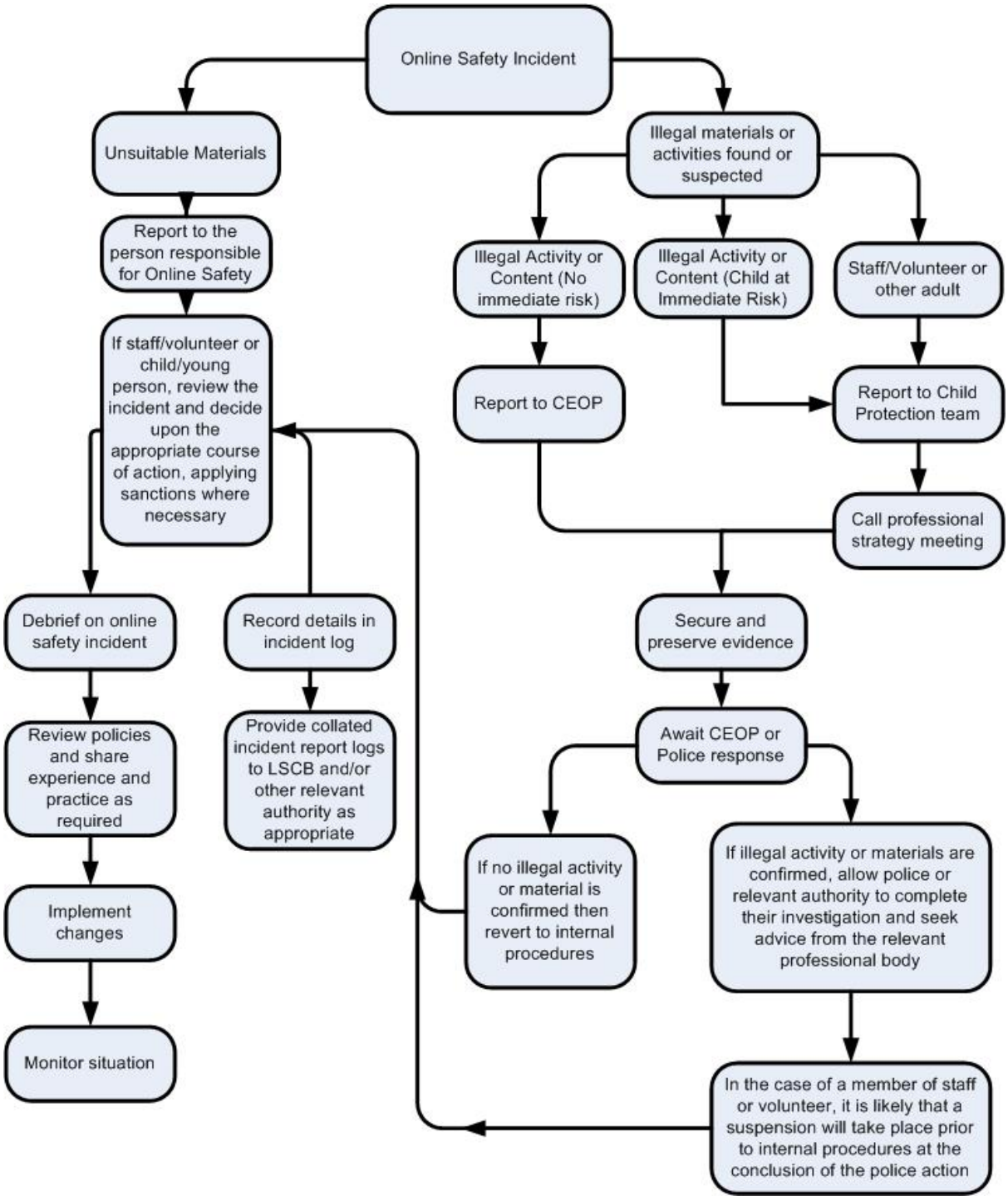
Responding to incidents of misuse

At Millwood we use the Online Safety Boost+ Incident Management tool to support staff to respond appropriately to reported incidents.

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
It is hoped that 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.

At Millwood we use the Online Safety Boost+ Incident Management tool to support staff to respond appropriately to reported incidents.

Training
A planned programme of formal online safety training is 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. External training is delivered at least every two years with updates and new information shared with staff as it becomes available

All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the relevant policies and procedures – eg safeguarding, E-safety, ICT acceptable use, staff code of conduct.

Training will be provided for any member of staff who identifies online safety as a training need within the appraisal process or training audit.

Designated Safeguarding Lead and ICT lead, when appointed, will receive regular updated through attendance and external training events and by reviewing documents released by relevant organisations

This Online Safety Policy and its updates will be presented to and discussed by staff in staff and team meetings.

Governors are able and encouraged to access training on e-safety through Governor Services

Millwood E-safety Incident Report

Incident Date:	Description of the occurrence	Immediate action	Further action	Legal Implication	Closed Date (Date that the incident is closed by the SMT)

Signed and dated by the person making the incident report.

Pass to the designated teacher for safeguarding.