Moor Hey School
Online Safety policy

School Mission Statement

Moor Hey School is an inclusive school where we work together to provide a caring and supportive environment to meet and celebrate the diverse abilities and needs of all our pupils, enabling them to fulfil their personal, social, moral and academic potential.

School Aims

- To provide a broad, balanced and relevant curriculum differentiated to meet individual needs.
- To encourage and promote understanding of each pupil's individual needs.
- To raise self-esteem through a positive approach to teaching & learning.
- To develop and enhance appropriate social skills in a range of contexts.
- To increase independence for life.

Introduction:

This policy applies to all members of the school community (including staff, pupils, parents/carers, governors, visitors and school community users).

Research has proven that use of technology brings enormous benefits to learning and teaching. However, as with many developments in the modern age, it also brings an element of risk. Whilst it is unrealistic to eliminate all risks associated with technology, the implementation of an effective Online Safety Policy will help children to develop the skills and confidence to manage potential risks and considerably reduce their impact.

Our Online Safety policy, as part of the wider safeguarding agenda, outlines how we will ensure our school community is prepared to deal with the safety challenges that the use of technology brings.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are also off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

This is pertinent to incidents of cyber-bullying, or other on line safety incidents covered by this policy, which may take place outside of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data and to report this to appropriate external sources e.g. Police. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate on line safety behaviour that take place out of school.

Our commitment to Online Safety:

At Moor Hey we discuss, monitor and review our Online Safety policy and procedures on a regular basis. Good practice suggests the policy should be reviewed annually or at most every two years.

We support staff in the use of ICT as an essential tool for teaching and learning and in the embedding of Online Safety across the whole school curriculum.

We also ensure, through our Computing and PSHE curriculums, that pupils understand the potential risks associated with the use of ICT, mobile and internet technologies; that all Online Safety concerns will be dealt with sensitively and effectively; that pupils feel able to and safe to report incidents or worries and concerns they have and that they abide by our school's Online Safety policy, including the Acceptable Use for pupils, staff and parents including the use of social media..

We provide opportunities for parents and carers to receive Online Safety education and information in order to enable them to support their children in developing good Online Safety behaviour, whilst keeping them safe on-line. The school will report back to parents and carers any Online Safety concerns. We encourage parents and carers to work with the school to uphold the Online Safety policy and also report any concerns they have.

We seek to learn from Online Safety good practice elsewhere and utilise the support of the Local Authority (LA) and relevant organisations when appropriate.

Purpose of the Online Safety Policy:

An effective whole school Online Safety Policy is one which provides clear direction to staff, pupils, parents and governors and others about expected codes of behaviour in dealing with Online Safety issues. An effective policy also makes explicit the school's commitment to the development of good practice and sound procedures.

For the purposes of this policy the term child will include all pupils aged 4-16.

At Moor Hey we are working with our staff, pupils and parents and carers to create a school community which values the use of new technologies in enhancing learning, encourages responsible use of ICT and follows agreed policies to minimise potential Online Safety risks.

Our Online Safety champion:

The Online Safety champion in school is Michelle Padgeon, Deputy Headteacher with DSL status. She will be supported in this role by the Headteacher Helen McLenahan and backup DSL and Assistant Headteacher Jackie Rawal.

The roles of these staff, including the Online Safety Champion are:

To be responsible for ensuring the development, maintenance and review of the Online Safety policy and associated policies and documents, including the Acceptable User Policies.

To ensure that the policy is implemented and that compliance with the policy is actively monitored.

To ensure all staff are aware of reporting procedures and requirements should an Online Safety incident occur and that this must be reported to the Online Safety Champion who will then inform the Headteacher or Assistant Headteacher in her absence.

To keep up-to-date with Online Safety issues, guidance from the Local Authority and through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP) and www.saferinternet.org and to share this information and guidance with the relevant stakeholders.

To share, provide or arrange Online Safety advice and training for all staff, parents and carers and governors.

To liaise closely with the school's Designated Senior Leaders and report all safeguarding issues accordingly.

Security and data management: ICT security is a complex subject that involves all technology users in the school. The school follows the Lancashire ICT Security Framework (published 2005) and this in line with the requirements of the Data Protection Act (1998).

Use of mobile devices:

Pupils

At school we use school-owned mobile devices including laptops, tablets, mobile phones, cameras and games consoles to provide enriching learning opportunities for our children. Children will only use such devices in the presence of an adult.

Children are permitted to bring their personal mobile devices into school since many travel a good distance to and from school and use their devices as a means of entertainment, whilst doing so. If a child brings a personal mobile device into school, it is collected each morning and locked in the school office then returned to the child at the end of the day. Children are aware that they are not to turn on their devices whilst in school, they are not permitted to use them to access the internet or actually use them to record staff or other children in school or on transport. If a child breaches this rule their parents or carers will be contacted and they will not be permitted to bring any personal device into school until advised otherwise.

The older pupils are permitted to use their mobile phones whilst at college in line with the individual college's mobile phone usage policy. The pupils are encouraged to use their devices in a safe and sensible manner.

Staff and all visitors

Staff and any visitor to school are not permitted to use their own personal mobile devices in the presence of a child and they must not use their devices to take images or other recordings of pupils, under any circumstances.

If staff and visitors wanting to use their device for personal use, during the school day (8.40am- 3.30pm) they must do so during the lunch period either in the staffroom, a non-teaching room (these are listed specifically in Appendix 1) or off the premises.

If staff need to use their mobile phone outside of this time, they must seek prior authorisation from a member of the Senior Leadership Team.

Staff and visitors must ensure that their devices are turned off during the school day (8.40am-3.30pm) so that they do not disturb the teaching and learning of children.

Site Supervisor

The exception to this is the school's site supervisor who carries a mobile device for safety reasons since he works alone, at times throughout the day. He needs to be able to contact the school office if he is working out of the building but on the school site and requires assistance and in cases of emergency. A mobile phone which doesn't contain a camera will be made available for use during these times.

He ensures that it is turned to silent when in the school building and during the school day (8.40am- 3.30pm) so that it does not disturb the teaching and learning of children.

Use of cameras and recording devices:

The guidance below is taken from the school's Child Protection Policy and must be followed. For the purpose of this document a camera refers to any mobile device which can take a picture.

Consent

Under the Data Protection Act 1998, the school seeks parental consent to take and use photographs or recordings for the purposes below. These consent forms are updated annually and consent is recorded on the pupil agreement document which is emailed to all staff and held centrally in the school office.

Staff are advised to check this form before taking and using photographs and recordings of pupils.

Class lists identify for staff, working in the school, any children whose photographs must not be taken.

Purpose of Photographs

Children throughout school might have their photographs taken by staff to:

- Provide evidence of progress for moderation, developmental records and recording pupil's work;
- Celebrate their achievements e.g. for displays in school.
- Create guidance notes e.g. for care plans or behaviour plans.

In addition photographs may be used to advertise or promote the school via the website, newspaper reports and the school prospectus.

The school seeks parental consent to take photographs or recordings for these purposes too.

When pupils work together photographs may contain other children in the background. Staff need to be aware of this and check contents before using the photographs.

When pupils are in photographs which are used for external accreditation and may need to be sent to examination boards for moderation purposes, the school will seek specific consent to send photographs or recordings for this purpose.

Specific permission will be sought from parents for images of pupils used on individual communication aids which may go home with a child.

All photographs must be taken on school equipment; no one is permitted to use their own mobile phones, cameras or recording devices.

Staff, visitors, volunteers and pupils are not permitted to use their own mobile phones or cameras or other recording devices to take or record any images of children for their own records during school time.

The school's cameras and memory cards must not leave the school setting unless on an educational visit.

<u>Parents/Carers</u>

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 school will take every opportunity to help parents understand these issues.

Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- their children's personal devices in the school (where this is allowed)

Under the Data Protection Act (1998), parents are entitled to take photographs of their own children on the provision that the images are for their own use. Including other children or for other purpose could constitute a potential breach of Data Protection legislation.

When parents attend school for events such as sports day or school productions they should be told that they should, as far as possible only film their own child and photographs can only be used for personal use, they should not be placed on social networking sites.

Parents are required to sign to say they intend to take photographs.

Photographs can only be taken in the presence of staff. Volunteers are not allowed to take photographs on school trips.

The Press

The press have special permissions in terms of Data Protection and may wish to name individual children to accompany a photograph this will only be allowed with written permission gained annually from parents.

Each time a photograph is to be used as a press release, confirmation of permission will be sought prior to photographs going to press.

Storage and Use of Photographs / Video:

School Photos must be printed/ uploaded in the school setting by staff and once done images should be immediately removed from the camera's memory and memory card.

Photographs required for reports or records may be placed on staff laptops, which are password protected, whilst the teacher or TA works upon the document. Once completed the photographs are deleted from the lap top.

Photographs will be stored on the school server which is password protected.

Photographs must be deleted when no longer required and as a guide this will be at the end of a key stage or when a child leaves the school.

Printing can only be done in the school setting. Individual printed photographs will remain in school until no longer required by school or sent home to the parent of the child who is depicted in the photograph.

The exception to this is school newsletters which are sent home to all parents.

Cameras, mobile phones and all types of recording devices are prohibited in changing or toilet areas.

There are two school mobile phones, which do not have cameras; these are located in the school office.

These phones are to be taken by a member of staff on all visits out of school.

They will have the school office number entered into the phone.

These phones are for emergency contact with school, staff on the visit, parents or the emergency services only.

If there is an allegation being made against a member of staff regarding the use of mobile phones, cameras or other recording devices, the LCC procedures for Managing Allegations against Staff will be followed.

Images of pupils must not be stored in Cloud storage.

When taking photographs all staff must maintain the dignity of the pupils; they should ensure that pupils are happy to be photographed and that they are suitably dressed and presented. All photographs must show pupils in a positive light.

Communication technologies:

Email

The Lancashire National Grid for Learning service is the school email system (Office 365). Personal email accounts should not be accessed in school time on school equipment.

Email accounts for children are only set up as part of planned curriculum activities. Pupils using email accounts are always supervised by staff.

As part of PSHE and Computing pupils are taught about the issues associated with use of email, cyber-bullying and sexting .

All users must be aware that they should not open attachments that they suspect may contain illegal content as they could inadvertently be committing a criminal act.

Pupils will be taught how to use the email safely and what to do if cyberbullying occurs. All staff are aware of the school’s policy and procedures with regard to peer on peer abuse.

Social Networks

Social Network sites allow users to be part of a virtual community. Current popular examples of these sites are Facebook, Twitter, Club Penguin and Moshi Monsters (for children). These sites provide users with simple tools to create a profile or page including basic information about themselves, photographs, and possibly a blog or comments. As a user on a social network site, you may have access to view other users' content, send messages and leave unmediated comments. Many social network sites are blocked by default through filtering systems used in schools, but these settings can be changed at the discretion of the Headteacher (See http://www.lancsngfl.ac.uk/lgfladvice/index.php for more details).

The use of social networking is included as part of staff induction, discussed regularly and outlined in the staff Acceptable Use Policy. When using social networks individuals should always conduct themselves in a professional manner. If content is made available on the web it is available for everyone to see and potentially remains there forever.

All staff must adhere to the following guidance:

If a social network site is used personally, details must not be shared with children and privacy settings should be reviewed regularly to ensure information is not shared automatically with a wider audience than intended.

Staff must not give personal contact details to pupils or parents/carers including mobile telephone numbers, details of any blogs or personal websites.

The content posted online should not:

- Bring the school into disrepute
- Lead to valid parental complaints
- Be deemed as derogatory towards the school and/or its employees

Staff must not access social networking sites for personal use during school hours (8:40am- 3:30pm).

Communications with parents, past pupils or siblings of pupils, especially if under the age of 18 should not occur. Children must not be added as 'friends' on any social network site.

The senior leadership team at Moor Hey School will not 'vet' prospective employees as such a practice can create an uneven playing field and lead to claims of discrimination.

Safeguarding issues

Communicating with both current and former pupils via social networking sites, emails or text messaging can lead to employees being vulnerable to serious allegations concerning the safeguarding of children and young people. (Refer to 'Guidance for Safer Working Practices for Adults Working with Children and Young People in Educational Settings')(September 2015)

Curriculum

Our PSHE and Computing curriculums both cover the acceptable use of social networking sites, emails and text messaging. We regularly discuss the safe and acceptable use of such communication technologies in school and we invite our local PCSO into school to keep our pupils updated on the law governing these.

Pupils to whom it is relevant will be educated in the safe use of social networking including cyber bullying, sexual exploitation, preventing radicalisation and sexting.

Instant Messaging or VOIP

Instant Messaging systems, e.g. text messaging, Skype, Facetime, are popular communication tools with both adults and children. Staff and pupils must not use school equipment to communicate with personal contacts e.g. through 'Facetime' on an iPad.

The school successfully uses text messaging to contact parents via Primary Contact, the security of messages and data is ensured through Primary Contact, which is a Lancashire approved communication company.

School administration staff, under supervision of the Headteacher and Deputy Headteacher are the only staff who can access the text service.

Websites and other online publications

This may include for example school websites, Social Network profiles, podcasts, videos, wikis and blogs. Information posted online is readily available for anyone to see and thus form an opinion about the school. Our school website communicates Online Safety messages to parents/carers. The website is only edited by administration staff and in agreement with the Headteacher or Deputy Headteacher.

Content is regularly reviewed by the Deputy Headteacher who has overall responsibility for what appears on the website.

Downloadable materials are in a read-only format (e.g. PDF)

Written consent from parents for photographs of their children used on the web site is obtained annually.

Data Protection

Personal data will be 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.

Following a number of "high profile" losses of personal data by public organisations, schools are likely to be subject to greater scrutiny in their care and use of personal data.

The school must ensure that:

It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.

Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".

There is a Data Protection Policy.

School is registered as a Data Controller for the purposes of the Data Protection Act (DPA)

Responsible persons are identified. Risk assessments are carried out. There are clear and understood arrangements for the security, storage and transfer of personal data. Data subjects have rights of access and there are clear procedures for this to be obtained. There are clear and understood policies and routines for the deletion and disposal of data. There is a policy for reporting, logging, managing and recovering from information risk incidents. There are clear Data Protection clauses in all contracts where personal data may be passed to third parties .There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.

- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.

- Transfer data using encryption and secure password protected devices.

When 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 (many memory sticks / cards and other mobile devices cannot be password protected)

- The device must offer approved virus and malware checking software

- The data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

Infrastructure and technology including filtering and virus protection:

The school ensures that the infrastructure and network are as safe and secure as possible by subscribing to the BT Lancashire Services (BTLS).

Internet content filtering is provided by default as part of the service level agreement with BT by Lightspeed systems. It is important to note that the filtering service offers a high level of protection. Pupils have restricted access provided by the filter however staff have a greater access via Lightspeed filtering, activated by their staff log-in. It is vital therefore that staff do not allow pupils access to their log-in details or leave their computer logged-in and left unattended.

Sophos Anti-Virus software is therefore included in the school's subscription to BTLS and is installed on administration computers in school. The computers on the curriculum network in school are secured by Symantec anti-virus software which are configured to receive regular updates.

Further information can be found at www.lancsngfl.ac.uk/esafety.

If any unsuitable content gets past the filter service it must be reported to the Online Safety champion and recorded in the Online Safety Incident Log. (APPENDIX 2)

Pupil access

Pupils are always supervised by a member of staff when accessing school digital equipment and online materials. They are taught about safe use of equipment and keeping safe on-line at school and at home. Pupils are taught the procedure to follow if they unwittingly view inappropriate content whilst online. Pupils who purposefully view inappropriate content will be subject to the school's discipline procedure, outlined in the Behaviour Policy. Any incidents are recorded in the Online Safety Incident Log. (APPENDIX 2)

Managing the network and technical support

The school works in partnership with BTLS (BT Lancashire Services) and RM (Research Machines) to ensure that the systems to protect pupils are reviewed and improved.

Illegal offences

Any suspected illegal material or activity must be brought to the immediate attention of the Headteacher who must refer this to external authorities, e.g. Police, CEOP. See the Online Safety Incident Escalation/ Procedure (APPENDIX 3)

Internet Watch Foundation (IWF)

Never personally investigate, interfere with or share evidence as you may inadvertently be committing an illegal offence.

It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident.

Always report potentially illegal content to the Internet Watch Foundation http://www.iwf.org.uk.

They are licensed to investigate – schools are not!

Examples of illegal offences are:

Accessing child sexual abuse images. Accessing non-photographic child sexual abuse images

Accessing criminally obscene adult content.

Incitement to racial hatred.

Accidental access to inappropriate content.

If any inappropriate content is accidentally accessed then the procedures to be followed are outlined in the Online Safety Incident Escalation/ Procedure (APPENDIX 3).

Briefly:

Staff - Minimise the webpage/turn the monitor off.

Enter the details in the Incident Log, report to school's eSafety champion or SLT then report to LGfL filtering services if necessary.

Child- Minimise the web page/turn off the monitor and tell an adult immediately.

Acceptable Use Policy (AUP):

An Acceptable Use Policy is intended to ensure that all users of technology within school are responsible and are protected from potential risk in their everyday use of ICT for educational, personal and recreational purposes. AUPs are provided for Staff and Visitors who are working in the classrooms and must be signed and adhered to by users before access to technology is allowed. Pupils have their own guidance to follow.

The school's Online Safety Policy and AUPs are reviewed annually in line with the policy monitoring cycle. Following the review staff are reminded of the importance of adhering to the AUP for themselves and pupils.

The Online Safety Policy and AUPs are available for parents and carers to read on the school website or hard copies are available from the office, on request.

Education and training:

In 21st Century society, both adults and children need to be digitally literate and aware of the benefits that the use of technology can provide. However, it is essential that children are taught to use technology responsibly, securely and safely, being able to recognise potential risks and knowing how to respond including how to respond to cyber-bullying and incitement to racial hatred.

The three main areas of online safety risk (as mentioned by OFSTED, 2013) that your school needs to be aware of and consider are:

Area of risk	Example of risk
Content: Children need to be taught that not all content is appropriate or from a reliable source.	Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse. Lifestyle websites, for example pro-anorexia/self-harm/suicide sites. Hate sites. Content validation: how to check authenticity and accuracy of online content
Contact: Children need to be taught that contact may be made using digital technologies and that appropriate conduct is necessary when engaging with these technologies.	Grooming Cyberbullying in all forms Identity theft (including 'frape' - hacking Facebook profiles) and sharing passwords
Conduct: Children need to be made aware that their personal online behaviour can increase the likelihood of, or cause harm to themselves and others.	Privacy issues, including disclosure of personal information, digital footprint and online reputation Health and well-being - amount of time spent online (internet or gaming). Sexting (sending and receiving of personally intimate images). Copyright (little care or consideration for intellectual property and ownership – such as music and film).

(Ofsted, 2013, Inspecting eSafety – guidance document)

At Moor Hey we teach this through our differentiated PSHE curriculum; our Computing curriculum; by staff continuously acting as a role model for pupils and by regularly referring to Online Safety when pupils are using digital technology. This is also personalised to the individual needs of pupils where necessary through Online Safety guidance if an incident occurs and it may form part of a pupil's IEP, if an identified need is recognised.

We also hold a focused whole school Online Safety day and assembly held in conjunction with national Online Safety initiative. We also have an annual focussed anti-bullying week held in conjunction with The Anti-Bullying Alliance awareness week in the autumn term. This addresses aspects of Online Safety including cyber-bullying.

We share Online Safety materials with parents through the school website and hold organised workshop for parents and pupils, which are led by our local PCSO officer and where the safe use of digital technology is reinforced along with the importance of reporting incidents. Our Online Safety Policy is available on our school website or hard copies can be obtained from the school office on request.

Online Safety – raising staff awareness:

New staff and visitors are inducted in the safe use of technology and are sign posted to the Online Safety Policy.

AUPs are provided for staff and visitors who are working in the classrooms and must be signed and adhered to by users before access to technology is allowed.

Online Safety – raising Governors' awareness:

Governors are part of our commitment to Online Safety and are represented on our Online Safety working group.

The Online Safety, Computing and Child Protection Policies are reviewed regularly according to the school's policy monitoring cycle and are discussed at the Governors' Committee meetings.

Governors receive specific Online Safety training delivered through school or the Local Authority Governor Services.

The Governor responsible for child protection is also kept up to date with developments and informed of any incidents by the DSL or Back up DSLs.

Evaluating the impact of the On line Safety Policy:

The Online Safety Policy will be reviewed annually according to the school's policy monitoring cycle or when an incident occurs that deems it necessary. All incidents will be monitored to check for any recurring patterns emerging and actioned accordingly. The Online Safety Policy will be amended to take account of this.

Written/Reviewed by: September 2017

Reviewed by: Mrs Padgeon

Date of next review: September 2018

APPENDIX 1

Rooms where staff are permitted to use mobile phones during the lunch period or for use outside of this time, with authorisation from a member of the SLT.

Staffroom

Headteacher's office

Deputy Headteacher's office

The meeting rooms

Becky's office

Janet's office

PPA room

Kitchen office

Site Supervisor's office in the prefab

Classroom Stock cupboards

APPENDIX 2

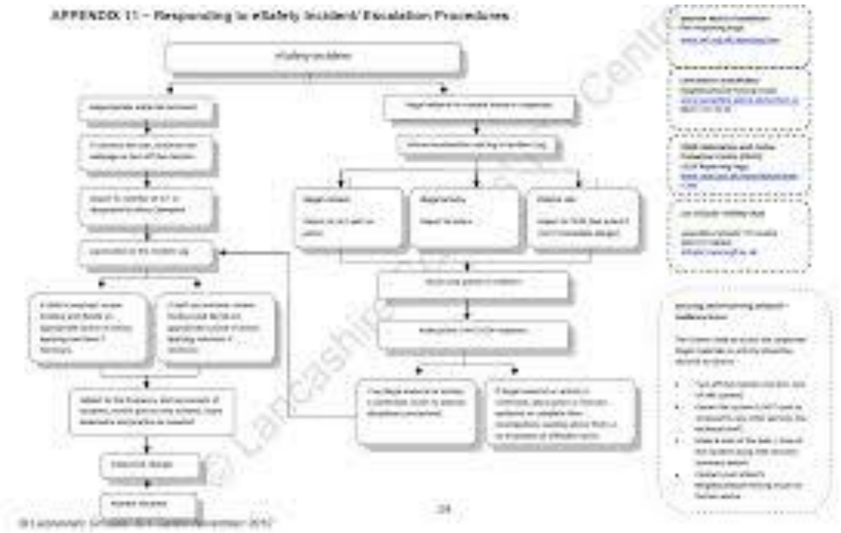
Online Safety Incident Log

All Online Safety incidents must be recorded by the School Online Safety Champion or designated person. This incident log will be monitored and reviewed regularly by the Headteacher and Chair of Governors. Any incidents involving Cyberbullying should also be recorded on the Integrated Bullying and Racist Incident Record Form 2 available via the Lancashire Schools Portal.

Date / Time of Incident	Type of Incident	Name of pupil/s and staff involved	System details	Incident details	Resulting actions taken and by whom (and signed)
EXAMPLE 3/9/15 10.50AM	EXAMPLE Accessing Inappropriate Website	EXAMPLE STAFF: PUPIL:	EXAMPLE Class 1 Computer	EXAMPLE Pupil observed by Teacher deliberately attempting to access inappropriate websites.	EXAMPLE Pupil referred to Online Safety champion and/ or Headteacher and given warning in line with sanctions in Behaviour Policy for first time infringement of AUP. Site reported to LGFL as inappropriate.

APPENDIX 3

Online Safety Incident/Escalation Procedure.


APPENDIX 11 – Responding to eSafety Incident/ Escalation Procedures

APPENDIX 4

Example of Typical Classroom eSafety

Rules (Lower school)

Our Golden Rules for Staying Safe with Computing

We only use the Internet when a trusted adult is with us.

We are always polite and friendly when using online tools.

We always make careful choices when we use the Internet.

We always ask a trusted adult if we need help using the Internet.

We always tell a trusted adult if we find something that upsets us.

APPENDIX 5

Example of Typical Classroom eSafety Rules

(Upper School)

Our Golden Rules for Staying Safe with Computing

We always ask permission before using the internet.

We only use the Internet when a trusted adult is around.

We immediately close/minimise any page we are uncomfortable with (or if possible switch off the monitor).

We always tell an adult if we see anything we are uncomfortable with.

We only communicate online with people a trusted adult has approved.

All our online communications are polite and friendly.

We never give out our own, or others', personal information or passwords and are very careful with the information that we share online.

We only use programmes and content which have been installed by the school.