




## Middlefield Community Primary School Online Safety Policy



	<b>Name of School</b>	Middlefield CP School
	<b>Policy review Date</b>	Oct 2016
	<b>Date of next Review</b>	Oct 2017
	<b>Who reviewed this policy?</b>	M.Hunter –Designated Safeguarding Person

This policy is part of the School's Statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection processes.

**“Nothing is more important than promoting  
the welfare of children and protecting them from harm”**

DFE, May 2016

(from the government's response to Alan Wood's, CBE – Review of the role and functions of Local Safeguarding Children Boards)

**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. An effective approach to online safety empowers a school to protect and educate the whole school community in their use of technology and establishes mechanisms to identify, intervene and escalate any incident where appropriate.**

DFE, May 2016

(from Annex C: Online Safety – Keeping Children Safe in Education)

adapted from, and with the kind approval of TRUSTnet/London Grid for Learning, Online Safety Policy - os.trustnet.pro

**TRUST**net

paul.bradshaw@si.liverpool.gov.uk 01.09.16



# Middlefield Community Primary School Online Safety Policy



## Contents

### 1. Introduction and Overview

- Rationale and Scope
- Roles and responsibilities
- How the policy is communicated to staff/pupils/community
- Handling complaints
- Reviewing and Monitoring

### 2. Education and Curriculum

- Pupil online safety curriculum
- Staff and governor training
- Parent awareness and training

### 3. Expected Conduct and Incident Management

### 4. Managing the IT Infrastructure

- Internet access, security (virus protection) and appropriate **filtering**
- Network management (user access, backup, curriculum and admin)
- Passwords policy
- E-mail
- School website
- Learning platform
- Social networking
- Video Conferencing

### 5. Data Security

- Management Information System access
- Data transfer
- Asset Disposal

### 6. Equipment and Digital Content

- Personal mobile phones and devices
- Digital images and video

adapted from, and with the kind approval of TRUSTnet/London Grid for Learning, Online Safety Policy - os.trustnet.pro



# Middlefield Community Primary School Online Safety Policy



- Appendices: All available on school website
- Acceptable Use Agreement (Staff, Volunteers and Governors)
  - Acceptable Use Agreements (Pupils – adapted for phase)
  - Acceptable Use Agreement including photo/video permission (Parents)
  - Protocol for responding to online safety incidents
  - <http://www.lgfl.net/esafety/Pages/policies-acceptable-use.aspx> - handling infringements
  - <http://www.digitallyconfident.org/images/resources/first-line-information-support-HQ.pdf> - page 23 onwards
  - Prevent: Radicalisation and Extremism
  - Data security: Use of IT systems and Data transfer
  - Search and Confiscation guidance from DfE
  - <https://www.gov.uk/government/publications/searching-screening-and-confiscation>

## 1. Introduction and Overview

### Rationale

#### The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Middlefield CP School with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff.
- Assist school staff working with children to work safely and responsibly with the Internet and other IT and communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use for the whole school community.
- Have clear structures to deal with online abuse such as online bullying [noting that these need to be cross referenced with other school policies].
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

adapted from, and with the kind approval of TRUSTnet/London Grid for Learning, Online Safety Policy - os.trustnet.pro



paul.bradshaw@si.liverpool.gov.uk 01.09.16



# Middlefield Community Primary School Online Safety Policy



- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

**The main areas of risk for our school community can be summarised as follows:**

## Content

- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

## Contact

- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

## Conduct

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)

## Scope

This policy applies to all members of Middlefield CP School community (including ALL staff, pupils/students, volunteers, parents/carers, visitors, community users) who have access to and are users of school IT systems, both in and out of Middlefield.

adapted from, and with the kind approval of TRUSTnet/London Grid for Learning, Online Safety Policy - os.trustnet.pro



# Middlefield Community Primary School Online Safety Policy



## Roles and responsibilities

Role	Key Responsibilities
Headteacher	<ul style="list-style-type: none"> <li>• Must be adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance.</li> <li>• To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding.</li> <li>• To take overall responsibility for online safety provision.</li> <li>• To take overall responsibility for data management and information security ensuring school's provision follows best practice in information handling and is compliant with the <a href="#">eight principles of the Data Protection Act 1998</a>.</li> <li>• To ensure the school uses appropriate IT systems and services including, a filtered Internet Service.</li> <li>• To be responsible for ensuring that <u>ALL</u> staff receive suitable training to carry out their safeguarding and online safety roles.</li> <li>• To be aware of procedures to be followed in the event of a serious online safety incident.</li> <li>• Ensure suitable 'risk assessments' are undertaken so the curriculum meets the needs of pupils, including the risk of children being radicalised.</li> <li>• To receive regular monitoring reports from the Online Safety Lead.</li> <li>• To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures, e.g. network manager.</li> <li>• To ensure Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety.</li> <li>• To ensure school that the school website includes relevant information and is compliant with the statutory requirements.</li> </ul>
Online Safety Lead/Designated Safeguarding Lead (this may be the same person)	<ul style="list-style-type: none"> <li>• Take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school's online safety policy/documents.</li> <li>• Promote an awareness and commitment to online safety throughout the school community.</li> </ul>

adapted from, and with the kind approval of TRUSTnet/London Grid for Learning, Online Safety Policy - os.trustnet.pro



paul.bradshaw@si.liverpool.gov.uk 01.09.16



## Middlefield Community Primary School Online Safety Policy



Role	Key Responsibilities
	<ul style="list-style-type: none"> <li>• Ensure that online safety education is embedded within the curriculum.</li> <li>• Liaise with school technical staff where appropriate.</li> <li>• To communicate regularly with SLT and the designated online safety Governor/committee to discuss current issues, review incident logs and appropriate filtering/monitoring issues and change control logs.</li> <li>• To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident.</li> <li>• To ensure that online safety incidents are logged as a safeguarding incident</li> <li>• Facilitate training and advice for <u>ALL</u> staff.</li> <li>• Oversee any pupil surveys/pupil feedback on online safety issues.</li> <li>• Liaise with the Local Authority and relevant agencies.</li> <li>• Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection concerns.</li> </ul>
Governors/Safeguarding governor (including online safety)	<ul style="list-style-type: none"> <li>• To ensure that the school has in place policies and practices to keep the children and <u>ALL</u> staff safe online.</li> <li>• To approve the Online Safety Policy and review the effectiveness of the policy.</li> <li>• To support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.</li> <li>• The role of the Online Safety Governor will include: regular review with the Online Safety Lead</li> </ul>
Computing Curriculum Lead	<ul style="list-style-type: none"> <li>• To oversee the delivery of the online safety elements of the Computing Curriculum.</li> </ul>
Network Manager/IT technician	<ul style="list-style-type: none"> <li>• To report all online safety related issues that come to their attention, to the Online Safety Lead.</li> <li>• To manage the school's computer systems, ensuring               <ul style="list-style-type: none"> <li>- school password policy is strictly adhered to.</li> <li>- systems are in place for misuse detection and malicious attack (e.g. keeping virus/malware/ransomware protection up to date).</li> <li>- access controls/encryption exist to protect personal and sensitive</li> </ul> </li> </ul>

adapted from, and with the kind approval of TRUSTnet/London Grid for Learning, Online Safety Policy - os.trustnet.pro



paul.bradshaw@si.liverpool.gov.uk 01.09.16



## Middlefield Community Primary School Online Safety Policy



Role	Key Responsibilities
	<p>information held on school-owned devices. - the school's policy on appropriate web filtering and monitoring is applied and updated on a regular basis.</p> <ul style="list-style-type: none"> <li>• To keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as required.</li> <li>• To ensure school technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the Online Safety Lead/DSL/Headteacher</li> <li>• To ensure appropriate backup procedures and disaster recovery plans are in place,</li> <li>• To keep up-to-date documentation of the school's online security and technical procedures.</li> </ul>
Data and Information Managers	<ul style="list-style-type: none"> <li>• To ensure that the data they manage is accurate and up-to-date.</li> <li>• Ensure best practice in information management. i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements.</li> <li>• The school must be registered with Information Commissioner.</li> </ul>
Teachers	<ul style="list-style-type: none"> <li>• To embed online safety in the curriculum.</li> <li>• To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant).</li> <li>• To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.</li> </ul>
All staff, volunteers and contractors.	<ul style="list-style-type: none"> <li>• To read, understand, sign and adhere to the school staff Acceptable Use Policy, and understand any updates - annually. The AUP is signed by new staff on induction.</li> <li>• To report any suspected misuse or problems to the Online Safety Lead.</li> <li>• To maintain an awareness of current online safety issues and guidance e.g. through relevant CPD.</li> <li>• To always model safe, responsible, respectful and professional</li> </ul>

adapted from, and with the kind approval of TRUSTnet/London Grid for Learning, Online Safety Policy - os.trustnet.pro



paul.bradshaw@si.liverpool.gov.uk 01.09.16



## Middlefield Community Primary School Online Safety Policy



Role	Key Responsibilities
	<p>behaviours in their own use of technology.</p> <p><b>Exit strategy</b></p> <ul style="list-style-type: none"> <li>• At the end of the period of employment returning any equipment or devices loaned by the school. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to log in and allow a factory reset.</li> </ul>
Pupils	<ul style="list-style-type: none"> <li>• Read, understand, sign and adhere to the Pupil /Student Acceptable Use Agreement, annually.</li> <li>• To understand the importance of reporting abuse, misuse or access to inappropriate materials.</li> <li>• To know what action to take if they or someone they know feels worried or vulnerable when using online technology.</li> <li>• To understand the importance of adopting safe, responsible and respectful behaviours and good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school.</li> <li>• To contribute to any 'pupil voice'/surveys that gathers information of their online experiences.</li> </ul>
Parents/carers	<ul style="list-style-type: none"> <li>• To read, understand and promote the school's Pupil Acceptable Use Agreement with their child/ren.</li> <li>• To consult with the school if they have any concerns about their children's use of technology.</li> <li>• To support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet, including social media and the school's use of photographic and video images</li> </ul>
External groups including Parent groups	<ul style="list-style-type: none"> <li>• Any external individual/organisation will sign an Acceptable Use Agreement prior to using technology or the Internet within school.</li> <li>• To support the school in promoting online safety.</li> <li>• To model safe, responsible, respectful and positive behaviours in their own use of technology.</li> </ul>

adapted from, and with the kind approval of TRUSTnet/London Grid for Learning, Online Safety Policy - os.trustnet.pro





# Middlefield Community Primary School Online Safety Policy



Communication:

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website and be available from the school on request.
- Policy to be part of school induction pack for new staff.
- Regular updates and training on online safety for all staff.
- Acceptable Use Agreements discussed with staff and pupils at the start of each year. Acceptable Use Agreements to be issued to whole school community, on entry to the school.

## Handling Incidents:

- The school will take all reasonable precautions to ensure online safety.
- Staff and pupils are given information about infringements in use and possible sanctions.
- Online Safety Lead to act as first point of contact for any incident.
- Any suspected online risk or infringement is reported to Online Safety Lead that day.
- Any concern about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer).

## Review and Monitoring

The Online Safety Policy is referenced within other school policies (e.g. Safeguarding and Child Protection Policy, Anti-Bullying Policy, PSHE, Computing Curriculum Policy).

- The Online Safety Policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school.
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school Online Safety Policy will be disseminated to all members of staff and pupils.

adapted from, and with the kind approval of TRUSTnet/London Grid for Learning, Online Safety Policy - os.trustnet.pro



# Middlefield Community Primary School

## Online Safety Policy



### 2. Education and Curriculum

#### Pupil online safety curriculum

This school:

- has a clear, progressive online safety education programme as part of the Computing Curriculum/PSHE and other curriculum areas as relevant. This covers a range of skills and behaviours appropriate to their age and experience;
- plans online use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- will remind pupils about their responsibilities through the Pupil Acceptable Use Agreement(s);
- ensures staff are aware of their responsibility to model safe, responsible, respectful and professional behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright;
- ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
- ensure pupils only use school-approved systems and publish within appropriately secure/age-appropriate environments.

#### Staff and governor training

This school:

- makes regular training available to staff on online safety issues and the school's online safety education program;
- provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the Online Safety Policy and the school's Acceptable Use Policies/Agreements.

#### Parent awareness and training

This school:

- provides online safety advice via the school's newsletter/website

adapted from, and with the kind approval of TRUSTnet/London Grid for Learning, Online Safety Policy - os.trustnet.pro



# Middlefield Community Primary School Online Safety Policy



## 3. Expected Conduct and Incident management

### Expected conduct

In this school, all users:

- are responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Policies/Agreements;
- understand the significance of misuse or access to inappropriate materials and are aware of the consequences;
- understand it is essential to reporting abuse, misuse or access to inappropriate materials and know how to do so;
- understand the importance of adopting safe, responsible and respectful online safety practice when using digital technologies in and out of school;
- know and understand school policies on the use of mobile and hand held devices including cameras;

### Staff, volunteers and contractors

- know to be vigilant in the supervision of children at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- know to take professional, reasonable precautions when working with pupils, previewing websites before use; using age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils;

### Parents/Carers

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the Online Safety Acceptable Use Agreement form;
- should know and understand what the school's 'rules of appropriate use for the whole school community' are and what sanctions result from misuse.

adapted from, and with the kind approval of TRUSTnet/London Grid for Learning, Online Safety Policy - os.trustnet.pro



# Middlefield Community Primary School Online Safety Policy



## Incident Management

In this school:

- there is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions;
- all members of the school are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes;
- support is actively sought from other agencies as needed (i.e. School Improvement Liverpool, UK Safer Internet Centre Helpline (0844 3814772/[helpline@saferinternet.org.uk](mailto:helpline@saferinternet.org.uk)), CEOP, Prevent Officer, Merseyside Police, IWF) in dealing with online safety issues;
- monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school;
- parents/carers are specifically informed of any online safety incidents involving young people for whom they are responsible;
- the Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law;
- we will immediately refer any suspected illegal material to the appropriate authorities – Merseyside Police, Internet Watch Foundation and inform the Local Authority.

## 4. Managing IT and Communication System

### Internet access, security (virus protection) and appropriate filtering and monitoring

This school:

- informs all users that Internet/email use is monitored;
- has filtered, secure broadband connectivity provided by TRUSTnet;
- uses LightSpeed Solutions which blocks sites that fall into categories (e.g. adult content, race hate, gaming). All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status;
- ensures network health through use of Sophos anti-virus software;
- Uses approved systems to send 'protect-level' (sensitive personal) data over the Internet.

adapted from, and with the kind approval of TRUSTnet/London Grid for Learning, Online Safety Policy - os.trustnet.pro



## Middlefield Community Primary School Online Safety Policy



- Uses encrypted devices or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site;
- Works in partnership with School Improvement Liverpool/Liverpool City Council Connect2ICT to ensure any concerns are communicated so that systems remain robust and protect pupils

### Network management (user access, backup)

This school

- Uses individual, audited log-ins for all users – TRUSTnet;
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services;
- Has additional local network monitoring/auditing software installed;
- Ensures the Systems Administrator/Network Manager is up-to-date with their technical knowledge;
- Has daily back-up of school data (admin and curriculum);
- Uses secure, 'Cloud' storage for data back-up that conforms to [DfE guidance](#);
- Storage of all data within the school will conform to the EU and UK data protection requirements; Storage of data online, will conform to the [EU data protection directive](#) where storage is hosted within the EU.

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's Online Safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. The same credentials are used to access the school's network / We also provide a different username and password for access to our school's network;
- All pupils have their own unique username and password which gives them access to the Internet and other services;
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins;
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to log off when they have finished working or are leaving the computer unattended;
- Ensures all equipment owned by the school and/or connected to the network has up to date virus/malware/ransomware protection;

adapted from, and with the kind approval of TRUSTnet/London Grid for Learning, Online Safety Policy - os.trustnet.pro



paul.bradshaw@si.liverpool.gov.uk 01.09.16



## Middlefield Community Primary School Online Safety Policy



- Makes clear that staff are responsible for ensuring that any computer/laptop/mobile device loaned to them by the school, is used only to support their professional responsibilities.
- Makes clear that staff accessing Local Authority systems do so in accordance with any corporate Liverpool City Council policies;
- Maintains equipment to ensure Health and Safety is followed;
- Ensures that access to the school's network resources from remote locations by staff is audited and restricted and access is only through school approved systems;
- Does not allow any outside agencies to access our network remotely except where there is a clear professional need and then access is audited, restricted and is only through approved systems;
- Has a clear disaster recovery system in place that includes a secure, remote off-site back up of data;
- This school uses secure data transfer.
- Ensures that all pupil level data or personal data sent over the Internet is encrypted.
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- All IT and communications systems are installed professionally and regularly reviewed to ensure they meet health and safety standards;

### Password policy

- This school makes it clear that staff and pupils must always keep their passwords private, must not share with others; If a password is compromised the school should be notified immediately.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private.
- We require staff to use secure passwords.
- We require staff using critical systems to use two factor authentication.

### E-mail

#### This school

- Provides staff with an email account for their professional use, and makes clear personal email should be through a separate account;
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.

adapted from, and with the kind approval of TRUSTnet/London Grid for Learning, Online Safety Policy - os.trustnet.pro



paul.bradshaw@si.liverpool.gov.uk 01.09.16



# Middlefield Community Primary School

## Online Safety Policy



- Will ensure that email accounts are maintained and up to date
- We use a number of technologies to help protect users and systems in the school, including desktop anti-virus products, plus direct email filtering for viruses.

### **Pupils:**

- Pupils are taught about the online safety and 'netiquette' of using e-mail both in school and at home.

### **Staff:**

- Staff can only use school e-mail systems on the school system.
- Staff will use the school e-mail systems for professional purposes.
- Access in school to external personal e mail accounts may be blocked.
- Never use email to transfer staff or pupil personal data. 'Protect-level' data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption.

### **School website**

- The Headteacher, supported by the Governing body, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- The school web site complies with statutory DFE requirements;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- Photographs published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;

### **Cloud Environments**

- Uploading of information on the schools' online learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas;
- Photographs and videos uploaded to the school's online environment will only be accessible by members of the school community;
- In school, pupils are only able to upload and publish within school approved 'Cloud' systems.

### **Social networking**

adapted from, and with the kind approval of TRUSTnet/London Grid for Learning, Online Safety Policy - os.trustnet.pro



# Middlefield Community Primary School Online Safety Policy



## Staff, Volunteers and Contractors

- Staff are instructed to always keep professional and private communication separate.
- Teachers are instructed not to run social network spaces for pupils use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.
- for the use of any school approved social networking will adhere to school's Communications Policy.

## School staff will ensure that in private use:

- No reference should be made in social media to students/pupils, parents/carers or school staff;
- Never post images or videos of pupils/students.
- School staff should not be online friends with any pupils/students or parents/carers of pupils/students.
- If they receive a friend request from a pupil/student or parent/carer they should decline the invite and inform their Line Manager.
- They do not engage in online discussion on personal matters relating to members of the school community;
- Personal opinions should not be attributed to the school and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute;
- Security and privacy settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

## Pupils:

- Are taught about social networking, safe, responsible, respectful and acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- Pupils are required to sign and follow our [age appropriate] pupil Acceptable Use Agreement.

## Parents:

- Parents are reminded about social networking risks and protocols through our parental Acceptable Use Agreement and additional communications materials when required.

adapted from, and with the kind approval of TRUSTnet/London Grid for Learning, Online Safety Policy - os.trustnet.pro





## Middlefield Community Primary School Online Safety Policy



- Are reminded that they need to ask permission before uploading photographs, videos or any other information about other people.
- Are encouraged to model safe, responsible and respectful use of social media for their children to emulate.
- As a school we believe that parents should be discouraged from using social media to criticise teaching staff and to make comments about our school and the community it serves. If you feel that you have any issues regarding your child's schooling, please make an appointment to come and talk to us. We are always happy to listen.

### CCTV

- We have CCTV in the school as part of our site surveillance for staff and student safety. The use of CCTV is clearly signposted in the school. We will not reveal any recordings without appropriate permission.

## 5. Data security: Management Information System access and Data transfer

### Strategic and operational practices

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- Staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are. We have listed the information and information asset owners.
- We ensure staff know who to report any incidents where data protection may have been compromised to.
- All staff are DBS checked and records are held in a single central record.

### Technical Solutions

- Staff have secure area(s) on the network to store sensitive files.
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 30 minutes idle time.
- We use the TRUSTnet USO AutoUpdate, for creation of online user accounts for access to broadband services and the TRUSTnet content.
- All servers are in secure, lockable locations and managed by DBS-checked staff.

adapted from, and with the kind approval of TRUSTnet/London Grid for Learning, Online Safety Policy - os.trustnet.pro



## Middlefield Community Primary School Online Safety Policy



- Details of all school-owned hardware will be recorded in a hardware inventory, including hardware on loan to named staff members.
- Details of all school-owned software will be recorded in a software inventory.
- Disposal of any equipment will conform to [The Waste Electrical and Electronic Equipment Regulations 2006](#) and/or [The Waste Electrical and Electronic Equipment \(Amendment\) Regulations 2007](#). [Further information](#) can be found on the Environment Agency website.
- Where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data.
- We are using secure file deletion software.

adapted from, and with the kind approval of TRUSTnet/London Grid for Learning, Online Safety Policy - os.trustnet.pro



# Middlefield Community Primary School

## Online Safety Policy



### 6. Equipment and Digital Content

#### Mobile Devices (Mobile phones, tablets and other mobile devices)

- Mobile devices brought into school are entirely at the staff member, pupils/students & parents or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- Mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile devices.
- No pupils/students should bring his or her mobile phone or personally-owned device into school. Any device brought into school will be confiscated.
- Mobile devices are not permitted to be used in certain areas within the school site, e.g. changing rooms and toilets. 'Mobile-free' signs to this effect are displayed.
- All mobile devices will be handed in at reception should they be brought into school.
- Personal mobile devices will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from Headteacher / SLT.
- Pupil/Student personal mobile devices, which are brought into school, must be turned off (not placed on silent) and stored out of sight on arrival at school. They must remain turned off and out of sight until the end of the day.
- The Bluetooth or similar function of a mobile device should be switched off at all times and not be used to send images or files to other mobile devices.
- Personal mobile devices will only be used during lessons with permission from the teacher.
- Mobile devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- No images or videos should be taken on mobile devices without the prior consent of the person or people concerned.
- Staff members may use their phones during school break times.
- All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any personal mobile device is to be avoided, except where it has been explicitly agreed by the Headteacher. Such authorised use is to be recorded. All mobile device use is to be open to monitoring scrutiny and the Headteacher is able to withdraw or restrict authorisation for use at any time, if it is deemed necessary.

adapted from, and with the kind approval of TRUSTnet/London Grid for Learning, Online Safety Policy - os.trustnet.pro



paul.bradshaw@si.liverpool.gov.uk 01.09.16



## Middlefield Community Primary School Online Safety Policy



- The School reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying. Staff mobiles devices may be searched at any time as part of routine monitoring.
- If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.

### Storage, Synchronizing and Access

#### **The device is accessed with a school owned account**

- The device has a school created account and all apps and file use is in line with this policy. No personal elements may be added to this device.
- PIN access to the device must always be known by the network manager.

#### **The device is accessed with a personal account**

- If personal accounts are used for access to a school owned mobile device, staff must be aware that school use will be synched to their personal cloud, and personal use may become visible in school and in the classroom.
- PIN access to the device must always be known by the network manager.
- Exit process – when the device is returned the staff member must log in with personal ID so that the device can be Factory Reset and cleared for reuse.

### Students' use of personal devices

- The School strongly advises that student mobile phones and devices should not be brought into school.
- The School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.
- If a student breaches the school policy, then the device will be confiscated and will be held in a secure place in the school office. Mobile devices will be released to parents or carers in accordance with the school policy.
- Phones and devices must not be taken into examinations. Students found in possession of a mobile device during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.

adapted from, and with the kind approval of TRUSTnet/London Grid for Learning, Online Safety Policy - os.trustnet.pro



paul.bradshaw@si.liverpool.gov.uk 01.09.16



## Middlefield Community Primary School Online Safety Policy



- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.
- Students will be provided with school mobile phones to use in specific learning activities under the supervision of a member of staff. Such mobile phones will be set up so that only those features required for the activity will be enabled.

### **Staff use of personal devices**

- Staff handheld devices, including mobile phones and personal cameras must be noted in school – name, make & model, serial number. Any permitted images or files taken in school must be downloaded from the device and deleted in school before the end of the day.
- Staff are not permitted to use their own mobile phones or devices in a professional capacity, such as for contacting children, young people or their families within or outside of the setting.
- Staff will be issued with a school phone where contact with students, parents or carers is required, for instance for off-site activities.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity, then it will only take place when approved by the senior leadership team.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes and then report the incident with the Headteacher / Designated Officer.
- If a member of staff breaches the school policy then disciplinary action may be taken.

adapted from, and with the kind approval of TRUSTnet/London Grid for Learning, Online Safety Policy - os.trustnet.pro



# Middlefield Community Primary School Online Safety Policy



## Digital images and video

### In this school:

- We gain annual parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form or when their daughter/son joins the school;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils;
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term, high profile use.
- The school blocks/filter access to social networking sites unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their Computing scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

adapted from, and with the kind approval of TRUSTnet/London Grid for Learning, Online Safety Policy - os.trustnet.pro



paul.bradshaw@si.liverpool.gov.uk 01.09.16