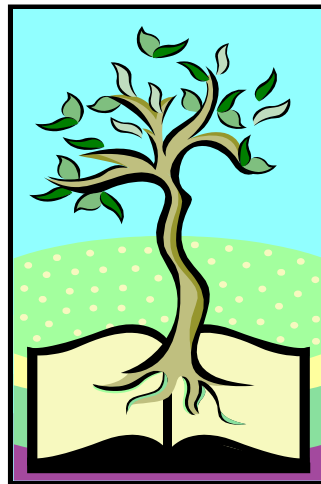


Online Safety Policy

Cadishead Primary School

February 2023



Contents

| | |
|---|-------------------------------------|
| Introduction | 4 |
| Policy Governance | 4 |
| Schedule for Review | 5 |
| Scope of the Policy | 6 |
| Roles and Responsibilities | 6 |
| Governors: | 6 |
| Headteacher and Senior Leaders: | 6 |
| Online Safety Coordinator/Officer: | 6 |
| Network Manager / Technical staff: | 6 |
| Teaching and Support Staff | 7 |
| Designated person for child protection/Child Protection Officer | 7 |
| Online Safety Committee | 7 |
| Students/pupils: | 7 |
| Parents/Carers | 8 |
| Community Users | 8 |
| Online Safety Education and Training | 9 |
| Education – students / pupils | 9 |
| Education & Training – Staff | 9 |
| Education and Training – Parents and Governors | 9 |
| Communication devices and methods | 10 |
| Unsuitable/inappropriate activities | 12 |
| Good practice guidelines | 15 |
| Email | 15 |
| Images, photos and videos | 16 |
| Internet | 17 |
| Mobile phones | 18 |
| Social networking (e.g. Facebook/ Twitter) | 19 |
| Webcams | 20 |
| Incident Management | 21 |
| Further information and support | 24 |
| Appendix 1 – Student/Pupil AUP | 25 |
| Student/pupil Acceptable Use Policy Agreement Template ... | Error! Bookmark not defined. |
| Student / Pupil Acceptable Use Agreement Form Template .. | Error! Bookmark not defined. |
| Appendix 2 – Staff, Volunteer, Community User AUP | 30 |

| | |
|---|-------------------------------------|
| School Acceptable Use Policy..... | Error! Bookmark not defined. |
| Appendix 3 – Use of Images Consent Form..... | 31 |
| Use of Digital / Video Images | Error! Bookmark not defined. |
| Appendix 4 –Supplementary Guidance: Common Facebook issues for schools and how to resolve them | 35 |
| Overview..... | 35 |
| Good Practice Guidelines and Incident Management | 36 |
| Further information and support for schools on Social Media Incidents..... | 37 |
| Contact details of various social network providers:..... | 38 |
| APPENDIX 4: Manchester Legal Services – Social Media, Schools and Parents. | 39 |

Introduction

This School Online Safety Policy Template is intended to help school leaders produce a suitable Online Safety policy document which will consider all current and relevant issues, in a whole school context, linking with other relevant policies, such as the Child Protection, Behaviour and Anti- Bullying policies.

The School Online Safety Policy applies to all members of the school community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems and mobile technologies, both in and out of school.

Policy Governance

Development, Monitoring and Review of this Policy

This Online Safety policy has been developed by a *Online Safety Committee* made up of:

| Position | Name(s) |
|---|---------------|
| <i>School Online Safety Coordinator / Officer</i> | Jack Weller |
| <i>Head Teacher</i> | Joanne Thomas |
| <i>Deputy Head Teacher</i> | Nicky Heggs |
| <i>Support Staff</i> | |
| <i>ICT Technical staff</i> | Colin Royle |
| <i>Governors</i> | |
| <i>Parents and Carers</i> | |
| <i>Community users</i> | |
| | |

Consultation with the whole school community has taken place through the following:

| Forum | Date (if applicable) |
|-------------------------------------|----------------------|
| <i>Staff meetings</i> | |
| <i>Governors meeting</i> | |
| <i>Parents evening</i> | |
| <i>School website / newsletters</i> | |
| | |
| | |
| | |

Schedule for Review

| | |
|---|---|
| <p>This Online Safety policy was approved by the <i>Governing Body / Governors Sub Committee</i> on:</p> | <p><i>February 2021</i></p> |
| <p>The implementation of this Online Safety policy will be monitored by <i>(the)</i>:</p> | <p><i>Jack Weller</i> <i>Online Safety Committee</i></p> |
| <p>Monitoring will take place at regular intervals:</p> | <p><i>Annually – every February</i></p> |
| <p>The <i>Governing Body / Governors Sub Committee</i> will receive a report on the implementation of the Online Safety policy generated by the monitoring group <i>Karen Gelder</i> at regular intervals:</p> | <p><i>Annually – every February</i></p> |
| <p>The Online Safety Policy will be reviewed <i>annually</i>, or more regularly in the light of any significant new developments in the use of the technologies, new threats to Online Safety or incidents that have taken place. The next anticipated review date will be:</p> | <p><i>February 2024</i></p> |
| <p>Should serious Online Safety incidents take place, the following external persons / agencies should be informed:</p> | <p><i>LA ICT Manager</i> <i>LA Safeguarding Officer</i> <i>Police Commissioner’s Office</i></p> |

Scope of the Policy

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

Roles and Responsibilities

The following section outlines the roles and responsibilities for Online Safety of individuals and groups within the school:

Governors:

- Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.

Headteacher and Senior Leaders:

- The Head Teacher is responsible for ensuring the safety (including Online Safety) of members of the school community
- The Head Teacher and another member of the Senior Leadership Team/Senior Management Team should be aware of the procedures to be followed in the event of a serious Online Safety allegation being made against a member of staff

Online Safety Coordinator/Officer:

- leads the Online Safety committee and/or cross-school initiative on Online Safety
- takes day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online Safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place.
- provides training and advice for staff
- receives reports of Online Safety incidents and creates a log of incidents to inform future Online Safety developments
- reports regularly to Senior Leadership Team

Network Manager / Technical staff:

The Managed Service provider (RM) is responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack

- that the school meets the Online Safety technical requirements outlined in the Salford City Council Security Policy and Acceptable Usage Policy and any relevant Local Authority Online Safety Policy and guidance
- that users may only access the school's networks through a properly enforced password protection policy

Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of Online Safety matters and of the current school Online Safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy/Agreement (AUP)
- they report any suspected misuse or problem to the *Online Safety Co-ordinator (Jack Weller) and the Child Protection Officer (Joanne Thomas), and if not present, the Senior Leader on site* for investigation/action/sanction

Designated person for child protection/Child Protection Officer

should be trained in Online Safety issues and be aware of the potential for serious child Protection issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- cyber-bullying

Online Safety Committee

Members of the Online Safety Committee will assist the Online Safety Coordinator/Officer with:

- the production, review and monitoring of the school Online Safety policy

Students/pupils:

- are responsible for using the school ICT systems and mobile technologies in accordance with the Student / Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems (nb. at KS1 it would be expected that parents/carers would sign on behalf of the pupils)
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

Parents/Carers

The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website/Learning Platform and information about national/local Online Safety campaigns/literature. Parents and carers will be responsible for:

- endorsing (by signature) the Student/Pupil Acceptable Use Policy
- accessing the school ICT systems or Learning Platform in accordance with the school Acceptable Use Policy.

Community Users

Community Users who access school ICT systems or Learning Platform as part of the Extended School provision will be expected to sign a Community User Acceptable Use Policy (AUP) before being provided with access to school systems.

Online Safety Education and Training

Education – students / pupils

Online Safety education will be provided in the following ways:

- A planned Online Safety programme will be provided as part of ICT/PHSE/other lessons and will be regularly revisited – this will cover both the use of ICT and new technologies in and outside school
- Key Online Safety messages will be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- Students/pupils will be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information
- Online safety scheme of work in Autumn 1 to include the children's AU policy
- Within themed weeks such as Anti-bullying week and Safer Internet day lessons

Education & Training – Staff

It is essential that all staff receive Online Safety training and understand their responsibilities, as outlined in this policy and the Training schedule appendix. Training will be offered as follows:

- *A planned programme of formal Online Safety training will be made available to staff. An audit of the Online Safety training needs of all staff will be carried out regularly. It is expected that some staff will identify Online Safety as a training need within the performance management process.*
- *All new staff will receive Online Safety training as part of their induction programme, ensuring that they fully understand the school Online Safety policy and Acceptable Use Policies*

Education and Training – Parents and Governors

It is essential that Governors and parents receive Online Safety awareness and/or training and understand their responsibilities. Training will be offered as follows:

































- *A planned programme of Online Safety awareness/ training will be made available to Governors and parents.*

Communication devices and methods

The following table shows the school's policy on the use of communication devices and methods.

Where it is indicated that the method or device is allowed at certain times, these are clearly outlined in the next table.

Completed in consultation with staff November 2022

| Communication method or device | Staff & other adults | | | | Students/Pupils | | | |
|---|---|---|---|---|---|---|---|---|
| | Allowed | Allowed at certain times | Allowed for selected staff | Not allowed | Allowed | Allowed at certain times | Allowed with staff permission | Not allowed |
| KEY |  |  |  |  |  |  |  |  |
| Mobile phones may be brought to school |  | | | | | |  | |
| Use of mobile phones in lessons | |  | | | | | |  |
| Use of mobile phones in social time |  | | | | | | |  |
| Taking photos or videos on personal mobile phones or other camera devices | |  | | | | | |  |
| Use of personal hand held devices eg PDAs, PSPs | |  | | | | | |  |
| Use of personal email addresses in school, or on school network | |  | | | | | |  |
| Use of school email for personal emails | | | |  | | | |  |
| Use of chat rooms / facilities | | | |  | | | |  |
| Use of instant messaging | |  | | | | | |  |
| Use of social networking sites | |  | | | | | |  |
| Use of blogs | |  | | | | |  | |
| Use of Class Dojo / 2simple |  | | | |  | | | |

| | | | | | | | | |
|-----------------------------|-------------------------------------|--|--|--|--|--|--|-------------------------------------|
| Use of school Twitter | <input checked="" type="checkbox"/> | | | | | | | <input checked="" type="checkbox"/> |
| Use of school Facebook page | <input checked="" type="checkbox"/> | | | | | | | <input checked="" type="checkbox"/> |
| Use of school YouTube | <input checked="" type="checkbox"/> | | | | | | | <input checked="" type="checkbox"/> |
| Use of class Skype Account | <input checked="" type="checkbox"/> | | | | | | | <input checked="" type="checkbox"/> |
| Use of Microsoft Teams | <input checked="" type="checkbox"/> | | | | | | | |



This table indicates when some of the methods or devices above may be allowed:














| Communication method or device | Circumstances when these may be allowed | |
|---|---|---|
| | Staff & other adults | Students/Pupils |
| Mobile phones may be brought to school | Any time | Only permitted in years 5 and 6. Handed in to teacher at start of day and picked up at the end of the day |
| Use of mobile phones in lessons | Only for emergencies / circumstances with permission | Never |
| Use of mobile phones in social time | During breaks or before and after school | Never |
| Taking photos or videos on personal mobile phones or other camera devices | Only with permission from SLT | |
| Use of personal hand held devices eg PDAs, PSPs | For professional / school use only with permission | Never |
| Use of personal email addresses in school, or on school network | During breaks or before and after school. Not for professional use | Never |
| Use of instant messaging | For school / professional use only with permission | Never |
| Use of social networking sites | For school / professional use – Facebook and Twitter blocked on school network. Youtube allowed (with a teacher login) for school / professional | Never |




| | | |
|--------------|-------------------------------|---|
| | use | |
| Use of blogs | For school / professional use | School approved blogs and only as directed by teacher |

Unsuitable/inappropriate 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 school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

Reviewed by Staff November 2022

| | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
|--|---|---|---|---|---|
| User Actions |  |  |  |  |  |
| child sexual abuse images | | | | |  |
| promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation | | | | |  |
| adult material that potentially breaches the Obscene Publications Act in the UK | | | | |  |
| criminally racist material in UK | | | | |  |
| Pornography | | | | |  |
| promotion of any kind of discrimination based on race, gender, sexual orientation, religion and belief, age and disability | | | | |  |
| promotion of racial or religious hatred | | | | |  |
| threatening behaviour, including promotion of physical violence or mental harm | | | | |  |

| | | | | | |
|--|--|---|---|---|--|
| 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 | | | |  | |
| Using school systems to run a private business | | | |  | |
| Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SCC and / or the school | | | |  | |
| Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions | | | |  | |
| Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords) | | | |  | |
| Creating or propagating computer viruses or other harmful files | | | |  | |
| Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet | | | |  | |
| On-line games (educational) | |  | | | |
| On-line games (non educational) | | | |  | |
| On-line gambling | | | |  | |
| Accessing the internet for personal or social use (e.g. online shopping, banking etc) | |  | | | |
| File sharing e.g. music, films etc | |  | | | |
| Use of social networking sites | | |  | | |
| Use of video broadcasting eg Youtube | |  | | | |
| Using external data storage devices (e.g. USB) that have not been encrypted (password protected and checked for viruses) | |  | | | |



This table indicates when some of the methods or devices above may be allowed:

| User Actions | Circumstances when these may be allowed | |
|--|--|--|
| | Staff & other adults | Students/Pupils |
| On-line games (educational) | Educational games only | Educational games only when directed / supervised by staff |
| Accessing the internet for personal or social use (e.g. online shopping, banking etc) | Only during break times or before and after school | Never |
| File sharing e.g. music, films etc | | Never |
| Use of social networking sites | Only teachers to access school accounts | Never |
| Use of video broadcasting eg Youtube | Only for showing educational videos access via teacher login | Never |
| Using external data storage devices (e.g. USB) that have not been encrypted (password protected and checked for viruses) | <p>Only for planning / resources / public documents</p> <p>Personal data / SEN / Child protection not to be stored on any device</p> <p>Photos / data on ipads are password protected – ensure strong password. Delete as soon as possible</p> | |

Good practice guidelines


Email



DO

Staff and students/pupils should only use their school email account to communicate with each other





Check the school Online Safety policy regarding use of your school email or the internet for personal use e.g. shopping



DO NOT

Staff: don't use your personal email account to communicate with students/pupils and their families without a manager's knowledge or permission – and in accordance with the Online Safety policy.

Images, photos and videos



DO

Only use school equipment for taking pictures and videos.

Ensure parental permission is in place.



Check the Online Safety policy for any instances where using personal devices may be allowed.

Always make sure you have the Headteacher/SLT knowledge or permission

Make arrangements for pictures to be downloaded to the school network immediately after the event.

Delete images from the camera/device after downloading.



DO NOT

Don't download images from organisation equipment to your own equipment.

Don't use your own equipment without Headteacher/SLT knowledge or permission – and in accordance with the Online Safety policy.

Don't retain, copy or distribute images for your personal use.

Internet



DO

Understand how to search safely online and how to report inappropriate content .



Staff and students/pupils should be aware that monitoring software will log online activity.

Be aware that keystroke monitoring software does just that. This means that if you are online shopping then your passwords, credit card numbers and security codes will all be visible to the monitoring technicians



DO NOT

Remember that accessing or downloading inappropriate or illegal material may result in criminal proceedings

Breach of the Online Safety and acceptable use policies may result in confiscation of equipment, closing of accounts and instigation of sanctions.

Mobile phones



DO

Use school equipment for contacting parents

Use school equipment for taking photographs

Store your phone away from view of pupils ie in your stock cupboard / bag

Make sure you know about inbuilt software/ facilities and switch off if appropriate.



Check the Online Safety policy for any instances where using personal phones may be allowed e.g. in an emergency

Staff: Make sure you know how to employ safety measures like concealing your number by dialling 141 first



DO NOT

Staff: Don't use your own phone without the Headteacher/SLT knowledge or permission.

Don't retain student/pupil/parental contact details for your personal use

Social networking (e.g. Facebook/ Twitter)

Schools should take into consideration the age of their pupils, and whether they are old enough to have accounts when including this guidance.

Best practice

DO

If you have a personal account, regularly check all settings and make sure your security settings are not open access.

Ask family and friends to not post tagged images of you on their open access profiles.

Consult a member of SLT if you are related to / or are personal friends with a parent and wish to accept them as friends on social media

Safe practice



Don't accept people you don't know as friends.

Be aware that belonging to a 'group' can allow access to your profile.

Poor practice

DO NOT

Don't have an open access profile that includes inappropriate personal information and images, photos or videos.

Staff:

- Don't accept students/pupils or their parents as friends on your personal profile.
- Don't accept ex-students/pupils users as friends.
- Don't write inappropriate or indiscrete posts about colleagues, students/pupils or their parents.

Webcams

Best practice

DO

Make sure you know about inbuilt software/ facilities and switch off when not in use.

Safe practice



Check the Online Safety policy for any instances where using personal devices may be allowed.

Always make sure you have the Headteacher/SLT knowledge or permission

Make arrangements for pictures to be downloaded to the school network immediately after the event.

Delete images from the camera/device after downloading.

Poor practice

DO NOT

Don't download images from organisation equipment to your own equipment.

Don't use your own equipment without Headteacher/SLT knowledge or permission – and in accordance with the Online Safety policy.

Don't retain, copy or distribute images for your personal use.

Incident Management

Dealing with unsuitable/inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities. The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in/or outside the school when using school equipment or systems. The school policy restricts usage as follows:

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).

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.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
 - Internal response or discipline procedures
 - Involvement by Local Authority
 - Police involvement and/or action
- **If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
 - incidents of ‘grooming’ behaviour
 - the sending of obscene materials to a child
 - adult material which potentially breaches the Obscene Publications Act
 - criminally racist material
 - promotion of terrorism or extremism
 - offences under the Computer Misuse Act (see User Actions chart above)
 - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

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

School actions & sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that

incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

Further information and support

For a glossary of terms used in this document:

<http://www.salford.gov.uk/d/salford-esafety-glossary-jan2012.pdf>

For Online Safety Practice Guidance for those who Work and Volunteer with, and have a Duty of Care to Safeguard Children and Young People:

<http://www.salford.gov.uk/d/Online-Safety-Practice-Guidance.pdf>

Safe Practice and Managing Allegations

Guidance for Safer Working Practice for Adults who Work with Children and Young People:

<http://www.partnersinsalford.org/sscb/safeppractice.htm>

R u cyber safe?

Online Safety tips about how to stay safe online:

<http://www.salford.gov.uk/rucybersafe.htm>

Please see attached:

Appendix 1 – Student/Pupil AUP

KS1



Cadishead Primary School



PUPIL ACCEPTABLE USE POLICY AGREEMENT

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers / tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of the computer, tablet and other equipment
- I will use the internet safely and it will help me learn
- I will be kind and respectful if I write a message or comment
- I will keep my usernames and passwords safe
- I will only communicate with people that I know
- I will never give out personal information (e.g. full name, address, telephone number)
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer / tablet

Name of child:

Class:

Signed (Child):

Signed (Parent / Carer):

Date:



PUPIL ACCEPTABLE USE POLICY

School Policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure:

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



I recognise that the school has a responsibility to maintain security:

- I will not use my own personal devices (mobile phones / USB devices etc) in school. If I bring a mobile phone to school, I will turn it off and hand it in to my teacher (Years 5 and 6 only).
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will not try to log in to personal social media sites or other personal accounts.

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

- I should ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not try to download copies (e.g. music, videos).
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

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

- I understand that school also has the right to take action against me if I am involved in incidents of inappropriate behaviour when I am out of school (e.g. cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network/internet, playtime, Star Time, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement.

If you do not sign and return this agreement, access will not be granted to school systems and devices.



PUPIL ACCEPTABLE USE POLICY AGREEMENT

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe - I will not share it or try to use any other person's username and password.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (e.g. names, addresses, email addresses, telephone numbers, age, gender, educational details)
- I will never arrange to meet anyone off-line that I have communicated with on-line.
- I will immediately report unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.
- I will not comment on the material or reply to the messages.

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

- I understand that our school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use our school's devices for on-line gaming, on-line gambling, file sharing, or video broadcasting (eg YouTube), unless I have permission to play on educational on-line game.

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

- I will respect others' work and property and will not access, copy, remove or alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.



Pupil Acceptable Use Agreement Form

This form relates to the pupil Acceptable Use Agreement.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems.

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

- I use school systems and devices (both in and out of school).
- I use my own equipment out of school in a way that is related to me being a member of our school e.g. communicating with other members of the school, accessing school email, website or programmes (e.g. Purple Mash or Mathletics).

Name of Pupil:

Class:

Signed (Pupil)

Signed (Parent / Carer)

Date:

Appendix 2 – Staff, Volunteer, Community User AUP



Cadishead Primary School



Staff and Volunteer Acceptable Use Policy Agreement

School Policy

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

This Acceptable Use Policy is intended to ensure:

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

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

Acceptable Use Policy Agreement

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

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, ipads, email etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.



- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

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

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

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

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.



- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings (submit request through RM support).
- I will not disable or cause any damage to equipment, or the equipment belonging to others.
- I will only transport planning, resources and public documents on external storage devices. Digital personal data will not be transferred outside the secure local network.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

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

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

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

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors / Directors and / or the Local Authority and in the event of illegal activities the involvement of the police.

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

Staff / Volunteer Name:

Signed:

Date:



Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website, class dojo / 2simple, in the public media and school social media (Facebook, Twitter and YouTube).

The school will comply with the Data Protection Act and request parents / carers permission before taking images of members of the school. We will also ensure that when images are published, children cannot be identified by the use of their names.

In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.

Parents / carers are requested to sign the permission form below to allow the school to take and use digital / video images of their children.

Digital / Video Images Permission Form

I agree to the school taking digital / video images of my child and using them through:

Newsletters, the school website, class dojo / 2simple and the public media. **YES / NO**

School social media accounts (Facebook, Twitter, YouTube) **YES / NO**

I agree to abide by these guidelines if I take digital / video images at a school event **YES / NO**

Parent / Carers Name:

Pupil Name:

Signed:

Date:



PHOTOGRAPHS AND VIDEOS OF CHILDREN

We would like to take **photographs and videos** of the pupils at our school. These photographs and videos may appear in printed publications, on our website and social media, or both.

The photographs and videos may appear in:

1. Printed publications
2. On our school website
3. In the local press
4. Our school Facebook and Twitter pages
5. On Class Dojo and /or 2Simple

Please note that websites can be viewed throughout the world, not just in the United Kingdom where UK law applies.

This form will begin from **Tuesday 1st December** and is valid until your child leaves the school or written confirmation is received from parents/carers changing permissions.

*If you would like to **opt out of this consent**, please contact the school office or your child's class teacher.*

Appendix 4 –Supplementary Guidance: Common Facebook issues for schools and how to resolve them

Overview

Salford City Council promotes the guidance from the Department for Education which advises headteachers and school staff on how to protect themselves from cyberbullying through the use of Social Media.

All forms of bullying (including cyberbullying) should be handled as a community issue for the whole school, in line with the advice in Salford's Online Safety Policy and documented in Schools Acceptable Use Policies. Every school should already have clear and understood policies in place that include the acceptable use of technologies by pupils and staff that address cyberbullying. It is important that schools make it clear that bullying of staff, whether by pupils, colleagues and parents, is unacceptable, and your existing policies may be updated to include issues arising from the widespread use of Social Media. Evidence indicates that one in five (21%) teachers have reported having derogatory comments posted about them on social media sites from both parents and children, and this guidance hopes to reduce and prevent these incidents.

Creating a good school-parent relationship can help create an atmosphere of trust that encourages parents to raise concerns in an appropriate manner. Part of this is making sure that parents and carers are aware and understand how to communicate with the school. Schools should also make clear that it is not acceptable for pupils, parents or colleagues to denigrate and bully school staff via social media in the same way that it is unacceptable to do so face to face.

Schools should develop clear guidance to help protect every member of the school community and to ensure that sanctions are appropriate and consistent. This will need to be effectively communicated to and discussed with employees, pupils and parents. Salford City Council has developed some model policy for schools to consider which should encourage all members of the school community including parents to use social media responsibly. A whole-school approach is recommended to develop new policy and practice effectively, ensuring that everyone is engaged in and aware of the schools approach to cyberbullying via Social Media. School governors with the head teacher and leadership team should audit existing policies (especially conduct, behaviour and ICT policies) and procedures to decide which need to be changed or adapted in order to include cyberbullying prevention and how to respond to incidents. *It is recognised that schools may have their own defined systems with which to manage and govern school policies, and managing social media issues could be embedded into existing policies rather than create new ones e.g. cyberbullying as part of anti-bullying and E-Safety etc.*

Unpleasant and abusive comments about schools or school staff. Some members of staff feel that comments posted about them are defamatory. The legal position is complex but does not offer a remedy in the majority of cases. In the case of Facebook, for example, the organisation is based in the USA where the courts generally do not enforce defamation judgements from the UK. In addition, local authorities (in whose name maintained schools would generally bring a claim)

are classed as 'organs of government' and cannot bring a legal claim in defamation. Manchester Legal Services have produced guidance on Social Media, Schools and Parents (see Appendices).

Good Practice Guidelines and Incident Management

- You should never respond or retaliate to cyberbullying incidents. You should document incidents appropriately and seek support from your senior leadership team, Online Safety Co-ordinator and/or Chair of Governors.
- Save evidence of the abuse; take screen prints of messages or web pages and record the time and date. Keeping good records of all cyberbullying incidents is essential to monitoring the effectiveness of your school's prevention activities, and to review and ensure the consistency of investigations, support and sanctions.
- Where the perpetrator is known to be a current pupil or colleague, the majority of cases can be dealt with most effectively through the school's own mediation and disciplinary procedures, in line with your Online Safety Policy and AUP.
- Where the perpetrator is known to be an adult, i.e. parent or other family member, in nearly all cases, the first action should be for a senior staff member to invite the person to a meeting to address their concerns, and if they have a reasonable complaint, to make sure they know how to raise this appropriately.
- Request that the person removes the offending comments. If online content is offensive or inappropriate, you need to ensure they understand why the material is unacceptable or offensive and request they remove it.
- If they refuse, it should be an organisational decision what to do next – either the Online Safety Co-ordinator, senior member of staff or you could report the matter to the social networking site if it breaches their terms.
- Most social networks have reporting mechanisms in place to report content which breaches their terms. If the person responsible has not been identified, or does not respond to requests to take down the material, the staff member should use the tools on the social networking site directly to make a report.
- If you are requesting they take down material that is not illegal, be clear to point out how it breaks the site's terms and conditions.
- You may wish to seek guidance or advice from the local authority regarding Facebook if your school firewall prevents access or whether the content is illegal.
- If the comments are illegal, i.e. threatening or abusive, of a sexual nature or constitute a hate crime, you or a representative from the school may consider contacting your local police officer or PCSO, or report via 101 directly.
- Repeated incidents of harassment or causing a person to fear that violence will be used against them could amount to a criminal offence. This should also be reported to police under the Protection from Harassment Act 1977.

Further information and support for schools on Social Media Incidents

Safe Practice and Managing Allegations

<http://www.partnersinsalford.org/sscb/safepractice.htm>

Salford City Council's advice about staying safe online.

<https://www.salford.gov.uk/rucybersafe.htm>

The Professional Online Safety Helpline is a free service for professionals and volunteers working with children and young people, delivered by the UK Safer Internet Centre. The helpline provides signposting, advice and mediation to resolve e-safety issues, such as protecting professional identity and online harassment.

The Safer Internet Centre has developed strategic partnerships with the key players in the internet industry. When appropriate, this enables the Professional helpline to seek resolution directly with the policy and safety teams at Facebook, Twitter, YouTube, Google, Tumblr, Ask.FM, Rate My Teacher and more.

School Employee Unions and Professional Associations

- Association of School and College Leaders (ASCL)

Phone: 0116 2991122

Web: www.ascl.org.uk

- Association of Teachers and Lecturers (ATL)

Phone: 020 7930 6441

Web: www.atl.org.uk

- National Association of Head Teachers (NAHT)

Phone: 01444 472472

Web: www.naht.org.uk

- NASUWT

Phone: 0121 453 6150

Web: www.nasuwt.org.uk

- National Governors' Association (NGA)

Phone: 0121 643 5787

Web: www.nga.org.uk

- National Union of Teachers (NUT)

Phone: 020 7388 6191

Web: www.teachers.org.uk

- Unison

Phone: 0845 355 0845

Web: www.unison.org.uk

- Voice: The Union for Educational Professionals

Phone: 01332 372 337

Web: www.voicetheunion.org.uk

Teacher Support Network
Phone: 08000 562 561
Web: www.teachersupport.info

Samaritans
Phone: 08457 90 90 90
Email: Jo@samaritans.org

Social networking sites (e.g. Bebo, FaceBook, MySpace)

Contact details of various social network providers:

Bebo: Reports can be made by clicking on a 'Report Abuse' link located below the user's profile photo (top left-hand corner of screen) on every Bebo profile page. Bebo users can also report specific media content (i.e. photos, videos, widgets) to the Bebo customer services team by clicking on a 'Report Abuse' link located below the content they wish to report. www.bebo.com/Safety.jsp.

Facebook: Reports can be made by clicking on the 'Report' link located on pages throughout the site, or by email to abuse@facebook.com
www.facebook.com/safety.

MySpace: Reports can be made by clicking on the 'Contact MySpace' link at the bottom of every MySpace page and selecting the 'Report Abuse' option. Alternatively, click on the 'Report Abuse' link located at the bottom of each user profile page and other user generated pages. Inappropriate images can be reported by clicking on the image and selecting the 'Report this Image' option. Additionally, school staff may email MySpace directly at schoolcare@myspace.com
www.myspace.com/safety.

Mobile phones

All UK mobile phone operators have nuisance call centres set up and/or procedures in place to deal with such instances. They may be able to change the number of the person being bullied. Mobile operators cannot bar a particular number from contacting a phone, but some phone handsets do have this capacity. Action can be taken against the bully's phone account (e.g. blocking their account) only with police involvement.

Contacts:

O2: ncb@o2.com or 08705214000.

Vodafone: 191 from a Vodafone phone or 08700700191 for Pay Monthly customers and 08700776655 for Pay as you Go.

3: Call 333 from a 3 phone or 08707330333.

Orange: Call 450 on an Orange phone or 07973100450 for Pay as you Go, or 150 or 07973100150 for Pay Monthly.

T-Mobile: Call 150 on a T-Mobile phone or 08454125000

APPENDIX 4: Manchester Legal Services – Social Media, Schools and Parents.

Manchester Legal Services has been receiving several requests from Schools for advice about comments made by parents on Facebook or other social networking sites.

These comments maybe upsetting for school staff and the purpose of this guidance is to suggest some approaches for dealing with them.

What can a School do in response to an offensive posting?

If a negative or offensive comment is made about the school or staff, the school's response will depend upon varying factors e.g. the nature of the posted comment and the type of site etc.

In most cases, the school can ask the parent to remove an offending item from a social networking site.

It should also be explained to the parent that social networking sites are not the appropriate forum to air any grievance and or complaints.

The school can also approach the website operator and ask them to remove it. Unfortunately, most social media operators e.g. Facebook are based in the US thus the UK has no legal jurisdiction.

Occasionally, the person posting the item is simply seeking attention and ignoring the posting may in fact be the best course of action. Pursuing the issue could actually worsen the situation because the material may then be circulated to a much wider audience. Another reasoning which the school may take is to ignore these postings or take steps to 'block' the sender if it is the sender's intent to deliberately target a member of staff or to try and involve the school in something that has nothing at all to do with them.

Threats of Violence or Racial Abuse

If the postings have threats of violence and/or racial abuse, this should be reported to the police. The Protection from Harassment Act 1977 provides that repeated incidents of harassment or causing a person to fear that violence will be used against them could amount to a criminal offence.

Is the content defamatory (libellous) enabling a legal course of action?

A school as a whole cannot be defamed; thus the comment, 'X school and its entire staff are useless at teaching' does not create a cause of action. The law in respect of defamation applies to an individual, a spoken comment is classed as slander and a written comment classed as libel.

The current law on libel which is already complex in itself when applied to traditional hardcopy publication becomes even more complex when applied to electronic and webs based postings (such as Facebook) which often involve not just the author and the website organiser but other contributors.

Even in a case of traditional libel, to pursue an action would involve an extremely lengthy and expensive process with no certainty of success or even if damages were awarded, there would be no certainty that the offender would have the means to pay.

Dealing with current problems and avoiding future ones

As technology continues to grow, practical approaches in dealing with these issues at school could include:

A 'whole school' approach

The school's anti-bullying policy is a good place for educating parents as well as pupils and staff about what constitutes acceptable use of internet or social

networking sites etc. Similarly, the school's behaviour policy with a message of acceptable standards is a good starting point.

Parents could also be reminded that School is trying to educate children about 'cyber bullying' and to protect pupils from becoming victims of such behaviour therefore posting negative or offensive comments on social networking sites sets a poor example and could lead children to believe that 'cyber bullying' is in some way acceptable. Further, if children have access to negative comments about their school, it could reduce their confidence in the school and this could damage their education.

The School's complaint policy

This should make clear that if parents have any issues or grievances, they should turn to the school in the first instance.