# Online Safety Policy

## Wombwell Park Street Primary School

Every Child Matters Academy Trust
*Children at the heart*

July 2023

Lyndsay Firth and Jordan Davison

Online Safety Policy

# Wombwell Park Street Primary School

# Online Safety and Computing Policy

## Introduction

The aim of this policy is to ensure that pupils learn how to use computers, modern technology and ICT in a safe manner. This policy outlines the steps that the school takes to ensure all pupils are protected from harm when using ICT within the school setting. The policy also proactively encourages children to develop a safe approach to using technology both in and outside of school.

We are committed to providing a caring, friendly and safe environment for all of our pupils so they can learn in a relaxed and secure atmosphere. Bullying of any kind is unacceptable at our school. If bullying does occur, all pupils should be able to tell and know that incidents will be dealt with promptly and effectively. We are a TELLING school. This means that anyone who knows that bullying is happening is expected to tell the staff.

Policy objectives:

- To promote a secure and happy environment free from threat, harassment and any type of bullying behaviour
- To take positive action to prevent bullying from occurring through a clear school policy on Personal and Social Development
- To show commitment to overcoming bullying by practising zero tolerance
- To inform pupils and parents of the school's expectations and to foster a productive partnership, which helps maintain a bully-free environment
- To make staff aware of their role in fostering the knowledge and attitudes which will be required to achieve the above aims.

## The Law

This policy has been written by the school, using government guidance. The policy is in place to promote positive learning, safeguarding and Data Protection. Although our policy is frequently updated, you can find the most up to date legislation documents (that are used to influence this policy) from the Department for Education website – www.education.gov.uk/schools.

## Roles and Responsibilities

The Headteacher and Deputy Headteacher, alongside the online safety leads (Lyndsay Firth and Jordan Davison) may:

- Ensure the policy is implemented, communicated and compliance with the policy is monitored
- Ensure staff training online safety is provided and updated annually as part of safeguarding training
- Ensure immediate action is always taken if any risks or dangers are identified ie reporting of inappropriate websites
- Ensure that all reported incidents of cyber bullying are investigated
- Ensure that all incidents of suspected radicalisation or incidents of individuals actively seeking out extremist material on the Internet are investigated

- Ensure appropriate web filtering software is used to protect users from potentially damaging/offensive material (DSLs will manage this in line with requirements in KCSIE 2023 around monitoring and filtering).

Teachers and Staff will:

- Keep passwords private and only use their own login details, which are stored securely
- Monitor and supervise pupils' internet usage and use of other IT resources
- Adhere to the Acceptable Use Agreement
- Promote online safety and teach online safety units as part of computing curriculum through the 'National Online Safety' programme and other resources.
- Engage in online safety training through the 'National Online Safety' programme.
- Only download attachments/material onto the school system if they are from a trusted source
- When capturing images, videos or sound clips of children, only use school cameras or recording devices unless the Headteacher grants special permission.

It is essential that pupils, parents/carers and the public have confidence in the school's decisions. This policy ensures that staff members use social media responsibly so that confidentiality of staff members and the reputation of the school are safeguarded. It is important that staff members must be conscious at all times of the need to keep their personal and professional lives separate.

Governors will:

- Ensure that the school is implementing this policy effectively
- Adhere to the Acceptable Use Agreement when in school
- Have due regard for the importance of online safety in school.

## Teaching and Learning

The 'National Online Safety' programme will be used to support teaching. The school will actively teach online safety, at an age appropriate level, to all pupils. Throughout the year, specific arrangements will be made to ensure that children are appropriately educated on social media, password control and cyberbullying amongst other topics. Online safety will be embedded throughout any learning where computing and technologies are used. The scheme 'NCCE' (National Centre for Computing Education) will also be used to teach online safety.

## Safe and Secure Systems

Internet access is regulated by HCC supplied filtered broadband connection which blocks access to unsuitable websites. Antivirus software has been installed on all computers and is to be maintained and updated regularly. Staff passwords must be strong passwords. Staff take responsibility for safeguarding confidential data saved to laptops, i.e. use of strong passwords. If personal data has to be saved to other media, e.g. memory sticks, it is to be encrypted. Staff with access to the ICT systems containing confidential and personal data are to ensure that such data is properly protected at all times. Teaching staff have remote access to the school server. This reduces the need for portable data storage and therefore increases security. Remote access is fully password protected and any laptops, which are taken off the school premises, are encrypted.

## Safe use of the Internet and Web Filtering

- All staff and pupils will have access to the internet through the school's network
- All staff and volunteers who use the school's IT equipment must read and sign the Staff acceptable Use Agreement
- All pupils must sign the Pupil Acceptable Use Agreement
- If staff come across a site that has inappropriate content, they must report this to the Headteacher

- If children encounter a site that contains inappropriate content they must report this to an adult who will then pass this information onto the Headteacher.

**Safeguarding - filtering and monitoring**

At WPSPS we utilise level 7 security to ensure the safety of our staff and children whilst using information technology. The provision is part of the solution offered by Talk-Straight Schools Broadband and is award winning since 2020. Each School is part of a contract with Schools Broadband and has a service level agreement in place governing all areas of Internet security to the schools. The firewall used is called FortiGate and is totally managed by Schools Broadband. The website filtering platform we utilise is called Netsweeper, which is also part of the level 7 security package we purchase. This works by using an agent which resides on every device that sits on the ECM Trust domain. This method allows ECM Trust ICT staff to complete management and surveillance over every device. The web filter is managed by Schools Broadband and partly managed by ECM's Head of ICT Services.

## The use of Email

All school staff are provided with a school email address. Staff should use this address when sending work-related emails. All emails should be professional in nature and staff should be aware that all emails can be retrieved at a later date should this be necessary. Staff emails should never be used to forward 'chain' or 'junk' email. Staff should not communicate with pupils or parents via their personal work email unless authorised by the Senior Leadership Team.

If staff are linking their school email address to portable devices, personal devices must be password protected. The content, or a preview of emails, should not be displayed on the portable device's lock screen.

## The School Website

The school website complies the statutory requirements set by the Department for Education. Images that include pupils must be appropriately selected and only used if parental consent has been given for the images to be posted online.

## Social Networking and Social Media

The school recognises that it has a duty to help keep children safe when they are accessing such sites at home, and to this end, the school will cover such issues within the curriculum. Pupils will not access social networking sites, e.g. Facebook, Twitter or Snapchat in school. They will be taught about how to stay safe when using such sites at home. School and class blogs are to run through the school website and are password protected.

## Staff Private use of Social Media

- No reference should be made in social media to students / pupils, parents / carers / school staff or issues / situations related to the school
- 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
- Security settings on personal social media profiles should be regularly checked to minimise risk of loss of personal information
- Teachers are instructed not to run social network spaces for student 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
- Staff are not permitted to maintain a Social Media relationship with any pupil, current or alumni until such time that the pupil turns 18.

## The use of Cameras, Video and Audio Recording Equipment

Staff may only use the school's photographic or video devices to support school trips and curriculum activities unless the Headteacher or Online Safety Leads have given authorisation. Photos should only be uploaded to the school system. They should never upload images to the internet unless specific arrangements have been agreed with the Headteacher, nor circulate them in electronic form outside the school. It is never acceptable to use photographic or video devices in changing rooms or toilets.

## Personal Mobile Devices

- Use of mobiles is discouraged throughout the school, particularly in certain areas. The areas which should be considered most vulnerable include: toilets and changing areas, including where children change for swimming
- The School reserves the right to search the content of any mobile or handheld devices on the school premises, where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence, or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring at the direction of the Headteacher.
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity unless authorised by the Senior Leadership Team.

## Management of Online Safety Incidents

- 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. MASH, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, IWF) in dealing with online safety issues
- Monitoring and reporting of online safety incidents takes place and contributes to developments in policy and practice in online safety within the school
- Parents/carers are specifically informed of 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 – Police, Internet Watch Foundation and inform the local MASH.

## Working in Partnership with Parents

Parents' attention will be drawn to the online safety policy through the school newsletter. The online safety policy will be available for all parents to access through the school website. All parents will be requested to sign an Acceptable Use Agreement on entry to the school.

## Protecting School Staff

In order to protect school staff, we ask that school issues and/or staff are not discussed using social media, Any concerns should be addressed with a member of staff from the school. The school will take action if there is any evidence of inappropriate comments regarding the school and/or staff have been placed on social media platforms or anywhere on the internet that is visible to the public.

## Safeguarding

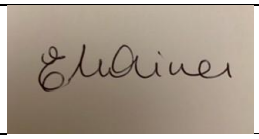
(See also Safeguarding and Behaviour Policies)

The Education and Inspections Act 2006 empowers the Headteacher to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the school's Behaviour Management Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online behaviour that take place out of school.

## Monitoring

This policy should be updated every year. The lead Governor is Mrs Elaine Oliver.

| | |
|---|---|
| **Chair of Governors** |  |
| **Headteacher** | |
| **Date** | 04.09.23 |

## Appendix

Appendix 1: Pupil and Parent Acceptable Use Agreement

Appendix 2: Staff and Volunteer Acceptable Use Agreement and Policy

Appendix 3: Response to an Incident of Concern

# Wombwell Park Street Primary School

Park Street, Wombwell, Barnsley. S73 0HS

Tel: 01226 752029

Email: parkstreet@ecmtrust.co.uk - Website: www.wombwellparkstreet.co.uk


**Wombwell Park Street Primary School**
**Computing and ICT Pupil Acceptable Use Agreement and Online-Safety Rules**

I will log on using my 'Classes/Team's' username and password.

I will immediately tell an adult if someone or something online has upset me or has made me feel unsafe or uncomfortable in any way.

I will ensure that I am always polite and responsible when using technology to contact other children and adults (who I know) online.

I will only upload content (images, videos, sounds or text) that is appropriate, truthful and kind and will not upset or cause harm to somebody else.

I will always keep my personal and private details to myself and I will never share these with anyone online when using any form of technology.

I know that the staff in school will check my use of technology and the internet to ensure I am following the above rules and will contact my parents/carers if any rule is broken.

I know the above rules are to keep me safe and therefore, I will always behave sensible when using technology because I am responsible for my own behaviour online.

**Think before you click!**

Dear Parent/Carer,

Computing and the use of ICT, including the internet, email, digital and mobile technologies is an essential part of learning at Wombwell Park Street. We expect all children to be responsible and safe users of the internet when using any form of technology.

Please read and discuss our Online Safety rules with your child and return the attached slip below. If you have any concerns or would like to discuss our school rules further, please contact our Computing and Online Safety Leads, Mrs Firth and Mr Davison.

---

**RE: Computing and ICT Pupil Acceptable Use Agreement and Online-Safety Rules**

We have discussed the Computing and ICT Pupil Acceptable Use Agreement and Online Safety Rules and …… (child's name) agrees to follow the Online Safety rules and to support the safe use of ICT and technology at Wombwell Park Street Primary School.

Parent/Carer Signature ……

Child signature……..

Class/Team…… Date……

Wombwell Park Street Primary School

Park Street, Wombwell, Barnsley. S73 0HS

Tel: 01226 752029

Email: parkstreet@ecmtrust.co.uk - Website: www.wombwellparkstreet.co.uk

**Wombwell Park Street Primary School**
**Computing and ICT Staff and Volunteer Acceptable Use Agreement and Online-Safety Rules**

I know that I must use the school Computing and ICT systems in a responsible way, to make sure there is no risk to my safety or to the safety and security of the Computing and ICT systems and other users.

For my Professional and Personal Safety

I understand that the rules set out in this agreement apply to use of the school Computing and ICT systems (e.g. laptops, iPads, email out of school).

I understand that the school can and may monitor my use of Computing and ICT systems, email and other digital communications.

I understand that the school Computing and ICT systems are primarily intended for the educational use and I will only use the systems for personal and recreational use within the policies set out by the school.

I will not disclose my username or password to another person, nor will I try to use another person's username and password.

I will immediately report any inappropriate, illegal or harmful material or incident.

I will only communicate with others in a professional manner, and I will not use aggressive or inappropriate language and I understand that others may have different opinions.

I will always ask permission before taking/publishing any content of others and will only do so in accordance with the school's policy on the use of digital content. I will not use personal devices to record content unless I have permission to do so.

I will not use social networking sites in school unless it is part of the curriculum.

I will only communicate with pupils/parents and carers using official school systems and any communication will be in a professional manner.

I will not participate in any online activity that may compromise my professional responsibilities or the reputation of the school.

When using personal devices (laptops, mobile phones, smartwatches, USBs etc) in school, I will only do so in accordance with the school's policies and I will follow the same rules set out in this agreement. I will ensure that such devices are protected by up to date anti-virus software and are free from viruses.

I will only open attachments to emails if the source is known and trusted.

I will not access, download or distribute any materials/content, which are inappropriate or illegal or cause harm to others.

I will not attempt to download or upload any content (unless I have permission) that might cause a delay in the school system, prevent others from carrying out their work or take up internet capacity.

I will not install or attempt to install any programmes on any machine, store programmes on a computer or alter computer settings without the permission of the Headteacher, Computing Leads and School IT Manager.

I will only save data onto an encrypted memory stick, encrypted school device or the school system.

I understand that the data protection policy requires any staff or pupil data, to which I have access, to be kept private and confidential. I will only disclose such information to an appropriate authority when it is deemed necessary by the law or by school policy.

**When using social networking sites and email outside of school**

I understand that when using social networking sites for personal use I have a professional responsibility. I will not make comments relating to school on any social networking sites and under no circumstances will I make reference to children, parents or staff.

I will never, under any circumstance, use social networking sites to communicate about school related issues. If anyone does attempt to contact me in relation to a school matter, I will refer

them to the appropriate channels through school and not answer them directly on the social networking site.

I will never form a Social Media relationship with any pupil, current or alumni until that pupil turns 18.

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

I understand that this Acceptable Use Poilcy applies to my work and use of the school's ICT equipment **and** my use of the school's ICT equipment out of school.

I understand that this Acceptable Use Policy applies to my use of persona; equipment in school and in situations related to my employment by the school.

I understand that if I fail to adhere and comply with the terms stated in the Acceptable Use Policy I could be subject to disciplinary action.

I have read and understood the above, and agree to use the school's ICT systems and equipment (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Signed……
Date……

# Response to an Incident of Concern

**Contacts**

- Barnsley Safeguarding Advisory Desk 0114 273 4934
- eSafety Project Manager (Sheffield) - Julia Codman 0114 293 6945
- South Yorkshire Police 101
- Child Exploitation and Online Protection Centre (CEOP)

**Online Safety Incident Occurs**

If a child is at immediate risk

Inform the Designated Child Protection Co-ordinator and follow school's child protection procedures

Seek advice from Safeguarding Advisory Service

Contact Barnsley Police (999) urgently if there is immediate danger

**Illegal Activity of Material found or suspected**

**Unsure**

**Inappropriate Activity or Material**

Consult with

Online Safety Project Manager

Content

Activity

Contact

Online Safety Project Manager

Report to Internet Watch Foundation (www.iwf.org.uk)

Or

Child

Staff

Contact Safeguarding Advisory Desk for advice

Report to CEOP

Child protection procedures and / or criminal action

Staff allegations procedures and / or criminal action

Activity

Child

Staff

Possible School Actions:

- Sanctions
- PHSE/citizenship
- Restorative Justice
- Anti Bullying
- Parental Work
- School support e.g. counselling, peer mentoring
- Request support / advice from eSafety Officer

Possible School Actions:

- Staff Training
- Disciplinary action
- School support e.g. counselling,
- Request support / advice from eSafety Officer

Content

Report to Filtering Manager and / or Schools Broadband Help Desk

**Review Schools eSafety policies and procedures, record actions in eSafety Incident log and implement any changes for future**

**Contact Details**

| |
|---|
| Schools Designated Child Protection Officer: Mrs Chloe Lawson |
| School Online Safety Co-ordinator: Mrs Lyndsay Firth and Mr Jordan Davison |