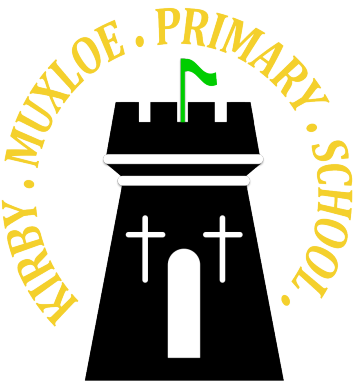
Kirby Muxloe Primary School



KMPS Online Safety Policy

Status: Voluntary
Date adopted by Trust Board:
Date for review: Autumn 2026

Key People

Designated Safeguarding Lead (DSL), with lead responsibility for filtering and monitoring	Sharon Jackson
Deputy Designated Safeguarding Leads / DSL Team Members	Elliot Howles Nick Holt Helene Fisher
Link governor for safeguarding	TBC
Link governor for webfiltering	Jordan Midgley
Curriculum leads with relevance to online safeguarding and their role	Georgina Chick - Computing Lead Rosie Coltman - PSHE Lead
Network manager / other technical support	James Crowhurst - Network Manager Schoolsbroadband - Internet & Filtering Provider

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The Trust Board

The trust board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The trust board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All members of the trust board will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 4)
- Appoint a filtering and monitoring governor to work closely with the DSL on the new filtering and monitoring standards.

3.2 The Headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

Details of the school's DSL and Deputy DSL's are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged using CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged using CPOMS and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety by conducting a yearly staff survey via Google Forms
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or trust board. This list is not intended to be exhaustive.

3.4 The ICT Manager

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged using CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff

All staff are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged using CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

Parents can seek further guidance on keeping children safe online on our school website and the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Hot topics Parent factsheet - Childnet International
- Healthy relationships – Disrespect Nobody

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 4).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum, our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

The introduction of the new relationships and sex education (RSE) curriculum was compulsory from September 2020. Under the new requirement, **all** schools have to teach: ▪ Relationships education and health education in primary schools

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The safe use of social media and the internet will also be covered in other subjects where relevant.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents via our website.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school's Behaviour Policy and Anti-bullying Policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers discuss cyber-bullying frequently with their classes.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information on cyber-bullying to parents so that they are aware of the signs, how to report it (see Anti-Bullying policy) and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the Anti-Bullying policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation .

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

All pupils and parents are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant. Staff will follow the agreement in the staff handbook.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

All users must not actively try to bypass the schools filtering system to access content that has been blocked by the schools filtering system. This includes the use of mobile phone hotspots. Mobile phone hotspots can only be used in exceptional circumstances with the permission of the headteacher. For example if the schools internet system is down and the school office need to access emails or the schools MIS.

Pupils should not actively try to connect a device to the guest wifi system to try and bypass pupil filtering.

Any breaches relating to attempts to bypass the schools filtering system will trigger disciplinary action in line with the schools behaviour and conduct policies.

It will be necessary to reinforce these as usual at the beginning of any school year but also to remind pupils that the same applies for any home learning that may take place in future periods of absence/ closure/quarantine etc.

More information is set out in the acceptable use agreements in appendices 1, 2, 3 and 4.

8. Messaging/Communication Systems

- Pupils at this school communicate with staff for learning purposes using our learning platform Seesaw.
- Pupils use our learning platform Seesaw for online homework and also if the school was to shut due to unforeseen circumstances teachers will use Seesaw to set online learning tasks for the children. This is monitored by the teaching staff and if any concerns arise they will follow the normal school procedures for reporting instances on CPOMs to the DSL.
- Staff at this school use the email system provided by Google For Education for all school emails. They never use a personal/private email account (or other messaging platform) to communicate with children or parents, or to colleagues when relating to school/child data, using a non-school-administered system.
- Staff at this school use Egress to communicate with other outside agencies when personal data about children is being communicated.
- The school office communicate with parents on behalf of staff using the schools communication system MyChildAtSchool provided by Bromcom.

Any systems above are centrally managed and administered by the school or authorised IT partner (i.e. they can be monitored/audited/viewed centrally; are not private or linked to private accounts). This is for the mutual protection and privacy of all staff, pupils and parents, supporting safeguarding best-practice, protecting children against abuse, staff against potential allegations and in line with UK data protection legislation.

Use of any new platform with communication facilities or any child login or storing school/child data must be approved in advance by the school and centrally managed.

Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).

Where devices have multiple accounts for the same app, mistakes can happen, such as an email being sent from or data being uploaded to the wrong account. If this is a private account used for communication or to store data by mistake, the DSL/Headteacher/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.

- Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff.
- Data protection principles will be followed at all times when it comes to all school communications, in line with the school Data Protection Policy and only using the authorised systems mentioned above.

9. Personal devices including wearable technology

Pupils may bring mobile devices into school, however these are tightly controlled and they must be handed in to the teacher at the start of the day. Pupils are not permitted to use personal mobile devices during the school day, including at before and after school clubs.

More information is set out in the schools separate mobile phone policy.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.

- All staff who work directly with children should leave their mobile phones on silent and only use them in private staff areas during school hours. See also the 'Digital images and video' section of this document and the school data protection cybersecurity policies. Child/staff data should never be downloaded onto a private phone. If a staff member is expecting an important personal call when teaching or otherwise on duty, they may leave their phone with the school office to answer on their behalf or ask for the message to be left with the school office.

- Volunteers, contractors, governors should leave their phones in their pockets and turned off. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the headteacher should be sought (the headteacher may choose to delegate this) and this should be done in the presence of a member staff.

- Parents are asked to leave their phones in their pockets and turned off when they are on site. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children. Parents are asked not to call pupils on their mobile phones during the school day; urgent messages can be passed via the school office.

10. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password or pin protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol) or a strong 6 digit pin is required.
- Ensuring encryption isn't removed from the device – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Not removing any school installed anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates unless instructed not to for operational reasons.

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

If staff have any concerns over the security of their device, they must seek advice from the school's ICT Manager.

11. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures and staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

12. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails and staff meetings).

The DSL and deputy DSLs will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Trust Board will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

13. Monitoring

It is vital that all members understand their responsibilities and those of others when it comes to filtering and monitoring. All staff have a key role to play in feeding back on potential issues.

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites (ask the DSL what appropriate filtering and monitoring policies are in place).

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular, extended school activities if relevant and remote teaching), supporting them with search skills, critical thinking (e.g. disinformation, misinformation and fake news), age appropriate materials and signposting, and legal issues such as copyright and data law.

It is vital that all staff recognise that online safety is a part of safeguarding (as well as being a curriculum strand of Computing, PSHE/RSHE and Citizenship).

General concerns must be handled in the same way as any other safeguarding concern.

Any suspected online risk or infringement should be reported to the online safety lead / designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson.

All staff will log behaviour and safeguarding issues related to online safety in CPOMS which will then be reviewed by DSLs.

Any concern/allegation 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).

The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF and Harmful Sexual Behaviour Support Service).

We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly concerning or breaks the law.

As schools, we are asked to follow the new DfE filtering and monitoring standards, which require us to:

- identify and assign roles and responsibilities to manage filtering and monitoring systems
- review filtering and monitoring provision at least annually
- block harmful and inappropriate content without unreasonably impacting teaching and learning
- have effective monitoring strategies in place that meet their safeguarding needs

ALL STAFF need to be aware of the changes and renewed emphasis and play their part in feeding back about areas of concern, potential for students to bypass systems and any potential overblocking. They can submit concerns at any point by emailing the ICT Manager and DSL and will be asked for feedback at the time of the regular checks which will now take place.

Staff will be reminded of the systems in place and their responsibilities at induction and start of year safeguarding as well as via Acceptable Use Policies and regular training reminders in the light of the annual review and regular checks that will be carried out.

At Kirby Muxloe Primary School:

- Web filtering is provided by SchoolsBroadband (TalkStraight) on school site and for school devices used in the home.
- Changes can be made by the ICT Manager and SchoolsBroadband.
- Overall responsibility is held by the DSL.
- Technical support and advice, setup and configuration are from the ICT Manager
- Regular checks are made half termly by the ICT Manager & DSL to ensure filtering is still active and functioning everywhere. These are evidenced by the testing spreadsheet and screenshots/ pdfs of filtering test results stored in the safeguarding shared drive.
- An annual review is carried out using the audit/review document (appendix 6) by the ICT Network Manager and DSL.

According to the DfE standards, “a variety of monitoring strategies may be required to minimise safeguarding risks on internet connected devices and may include:

• physically monitoring by staff watching screens of users

• live supervision by staff on a console with device management software

• network monitoring using log files of internet traffic and web access

• individual device monitoring through software or third-party services

At Kirby Muxloe Primary School, we use

- Apple Classroom to monitor pupil iPad screens.

- Physical monitoring of pupil iPad screens by staff moving around the room.
- Daily log file reporting from Schoolsbroadband
- Live email alerts to the ICT Network Manager and DSL on certain keywords including words linked to but not limited to prevent, IWF watchlist and pornography provided by Schoolsbroadband.
- Live email alerts to the ICT Network Manager and DSL on certain URL/Website access linked to but not limited to prevent, IWF watchlist and pornography provided by Schoolsbroadband.

This policy will be reviewed every 2 years. At every review, the policy will be shared with the governing body.

14. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy
- Anti-bullying policy

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/ CARERS	
Name of pupil:	
When I use the school's ICT systems (like computers) and get onto the internet in school I will: • Ask a teacher or adult if I can do so before using them • Only use websites that a teacher or adult has told me or allowed me to use • Tell my teacher immediately if: • ○ I click on a website by mistake ○ I receive messages from people I don't know ○ I find anything that may upset or harm me or my friends • Use school ipads for school work only • I will be kind to others and not upset or be rude to them • Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly • Only use the username and password I have been given • Try my hardest to remember my username and password • Never share my password with anyone, including my friends. • Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer • Save my work on the school network • Check with my teacher before I print anything • Log off or shut down a computer when I have finished using it **I understand that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/ CARERS	
Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy **When I use the school's ICT systems (like computers) and get onto the internet in school I will:** • Always use the school's ICT systems and the internet responsibly and for educational purposes only • Only use them when a teacher is present, or with a teacher's permission • Keep my username and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others • Always log off or shut down a computer when I'm finished working on it **I will not:** • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Log in to the school's network using someone else's details • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **If I bring a personal mobile phone or other personal electronic device into school:** • I will hand the mobile in to the teacher at the start of the day and collect it at the end. • I will not use it without a teacher's permission. • I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online **I understand that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 3: Staff Mobile Device and Internet Professional Conduct Agreement

Kirby Muxloe Primary School

Mobile Device and Internet Professional Conduct Agreement

By signing this agreement you agree to abide by the protocols and procedures outlined below. This agreement may be subject to change, pending reviews. If so, staff will be given a new version and asked to re-sign.

1. Device Ownership & Care
    1. Your device, and all accessories, remain the property of Kirby Muxloe Primary School and you agree to return the device, should you cease employment with the school or at any time by specific request of the school.
    2. A case has been provided for you that will protect the device. If you remove the device from the case or place it in your own case then you will be liable for any damage costs.
    3. While the device is offsite it will be insured by your home insurance. If you wish to use the device away from your home please ensure your home insurance covers this.
2. Device Professional Use
    1. The device is provided to enhance and support digital working practices. As a result, it should be used in a sensible professional capacity. Personal Apps may be installed but all reasonable care should be taken so that a child working on your device cannot access these apps (Use guided access etc). These Apps should only be used in your own free time.
    2. This device must not be used in a way that would bring the school into disrepute, contravene school disciplinary rules, professional expectations or break the law.
    3. Staff should not permit persons other than school staff access to the device and the potentially sensitive material that it provides access to.
3. Application / 'App' Guidance
    1. Should staff wish to purchase Apps for use on their device to use at school, they should seek authorisation first. Some Apps which are useful for all staff can be brought through a Volume Purchase Programme and centrally distributed.
    2. Any Apps installed by you for Personal or School use will not have technical support from the school.
4. Security & Backup
    1. It is the responsibility of staff to back-up their own data on their device through iCloud and Google Drive. Kirby Muxloe Primary School will not be responsible for loss of data.
    2. The device must have a security passcode on which is enabled.
    3. Device management systems should not be removed from the device.
    4. Kirby Muxloe Primary Schools device management system will be used to monitor the device and carry out remote operations as and when required.
    5. Should your device become lost, stolen or damaged, it is your responsibility to report this immediately to all relevant parties.

5. Health and safety

    1. You are provided with a stand and keyboard. Please use these when using the device for prolonged periods to minimise reflection and to ensure wrist and forearm support.

6. When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

1. Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
2. Use them in any way which could harm the school's reputation
3. Access social networking sites or chat rooms unless for school related reasons
4. Use any improper language when communicating online, including in emails or other messaging services
5. Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
6. Share my password with others or log in to the school's network using someone else's details
7. Take photographs of pupils without checking with teachers first
8. Share confidential information about the school, its pupils or staff, or other members of the community
9. Access, modify or share data I'm not authorised to access, modify or share

Promote private businesses, unless that business is directly related to the school

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Device: _____

Accessories: _____

Serial Number: _____

Asset ID: _____

I have read and understand the agreement

Signed: _____ Date: ___/___/___

Print: _____ Date: __/___/____

Appendix 4: Acceptable use agreement (trust board, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR TRUST BOARD, VOLUNTEERS AND VISITORS	
Name of trust board/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms unless for school related reasons • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with teachers first • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (trust board/volunteer/visitor):	**Date:**

Appendix 5: Online safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 6: Audit/Review Tool

Internet Filtering and Monitoring Standards for Schools and Colleges – Review / Check

School……..……..

Reviewer/s…….. Date…….

Oversight and management	Yes / No	Details, evidence or actions needed
Have you assigned a member of the senior leadership team and a governor, to be		
Have you identified and assigned the roles and responsibilities of staff and third parties, eg,		
Has the DSL and SLT done the following…?		
· procured filtering and monitoring systems		
· documented decisions on what is blocked or allowed and why		
· reviewed the effectiveness of your provision		
· overseen filtering and monitoring reports		
Has the DSL/SLT ensured that all staff…?		
· are appropriately trained		
· understand their role eg in reporting concerns		
· follow policies, processes and procedures		
· act on reports and concerns		
Is there a need for system specific training and/ or support from your filtering and monitoring		
Does the DSL receive and action…?		
· filtering and monitoring reports		
· online safeguarding concerns		
· checks to filtering and monitoring systems ie is it working as it should?		
Does the IT service provider…?		
· procure a filtering and monitoring system		
· carry out checks		
· identify risk for your school community		
· carry out reviews		
· maintain the filtering and monitoring system		
· provide filtering and monitoring reports to DSL/SLT		

· complete actions following concerns or checks		
Filtering and monitoring review	Yes / No	Details, evidence or actions needed
· Do governors ensure a review is carried out at least annually or following a safeguarding		
· Does the DSL, SLT, IT provider and responsible governor all have a role in		
· Is the review recorded for reference and available to inspectors if requested?		
· Does the review focus on the current provision, any gaps and the needs of your		
Comment on the following aspects as part of your review		
· the risk profile of your pupils, including their age range, pupils with special educational		
· what your filtering system currently blocks or allows and why		
· any local outside safeguarding influences, such as county lines		
· any relevant safeguarding reports		
· the digital resilience of your pupils		
· teaching requirements, for example, your RHSE and PSHE curriculum		
· the specific use of your chosen technologies, including whether Bring Your Own Device		
· what related safeguarding or technology policies you have in place		
· what checks are currently taking place and how resulting actions are handled		
What actions need to be taken as a result of the review? eg, in the following areas… · related safeguarding or technology policies and procedures · roles and responsibilities · training of staff · curriculum and learning opportunities · procurement decisions		
Have your checks included…?		
· School owned devices and services including off-site		
· Geographical areas across the school site		
· User groups eg teachers, pupils, guests		
· Whether staff know how to report and record concerns		
· Whether filtering and monitoring works on all new devices before release to pupils or		
· A review of blocklists and whether they are able to be modified if needed		
· Use of the SWGfL testing tool for illegal and adult content - testing tool		

Have you kept a log of your checks including…?		
· Date and time undertaken		
· Who did the check		
· What was tested or checked?		
· Resulting actions		
Filtering of harmful and inappropriate content	Yes / No	Details, evidence or actions needed
· Does your filtering system block harmful and inappropriate content without impacting		
· Do you need system specific training and support from your IT provider to enable the		
Is your filtering provider…?		
· a member of Internet Watch Foundation (IWF)		
· signed up to Counter-Terrorism Internet Referral Unit list (CTIRU)		
· blocking access to illegal content including child sexual abuse material (CSAM)		
Is your filtering system working, up to date and applied to all…?		
· users, including guest accounts		
· school owned devices		
· devices using the school broadband connection		
Does your filtering system…?		
· filter all internet feeds, including any backup connections		
· be age and ability appropriate for the users, and be suitable for educational settings		
· handle multilingual web content, images, common misspellings and abbreviations		
· identify technologies and techniques that allow users to get around the filtering such		
· provide alerts when any web content has been blocked		
Does your filtering system work on mobile or app technologies?		
Does your filtering system allow you to identify…?		
· device name or ID, IP address, and where possible, the individual		
· the time and date of attempted access		
· the search term or content being blocked		
Do all staff know how to report and record if…?		
· they witness or suspect unsuitable material has been accessed		
· they can access unsuitable material		

· they are teaching topics which could create unusual activity on the filtering logs		
· there is failure in the software or abuse of the system		
· there are perceived unreasonable restrictions that affect teaching and learning		
· they notice abbreviations or misspellings that allow access to restricted material		
Effective Monitoring Strategies	Yes / No	Details, evidence or actions needed
· Which monitoring strategy does your school use? 1. Physical monitoring by staff of screens 2. Live supervision on a console with device management software		
· Is monitoring working as expected by providing reporting on pupil device activity?		
· Is there a need for training on specific systems?		
· Does your monitoring system pick up incidents urgently through alerts or		
· Does the DSL take lead responsibility for safeguarding matters picked up?		
· Is monitoring data received in a format that your staff can understand?		
· Are users identifiable to the school or college, so concerns can be traced back to		
· Are monitoring procedures reflected in AUPs, online safety and safeguarding policies?		