Millfields First School

Online safety policy

Date reviewed: March 2023

Date of next review: March 2024

Chair of Governors (signature)

Head Teacher (signature)

Content

Background and rationale

The potential that technology has to impact on the lives of all citizens increases year on year. This is probably even more true for children and young people, who are generally much more open to developing technologies than many adults. In many areas, technology is transforming the way that children and young people learn and are taught. At home, technology is changing the way children and young people live and communicate, and the activities in which they choose to partake; these trends are set to continue.

While developing technology brings many opportunities, it also brings risks and potential dangers of which these are just a few:

- Access to illegal, harmful or inappropriate images or other content
- Allowing or seeking unauthorised access to personal information
- Allowing or seeking unauthorised access to private data, including financial data
- The risk of being subject to grooming or radicalisation by those with whom they make contact with on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive or addictive use which may impact on social and emotional development and learning.

This policy sets out how we strive to keep pupils safe with technology while they are in school. We recognise that children and young people are often more at risk when using technology at home (where often no controls over the technical structures are put in place to keep them safe) and so this policy also sets out how we educate them about the potential risks and try to embed appropriate behaviours. We also explain how we attempt to inform those people who work with our pupils beyond the school environment (parents, friends and the wider community) to be aware and to assist in this process.

With the recent increase of children accessing their learning from home, this document also explains how we equip and prepare children for safe and appropriate use of technology at home to support their education.

Our online-safety policy has been written from a template provided by Worcestershire County Council which has itself been derived from that provided by the South West Grid for Learning.

Section A - Policy and leadership

This section begins with an outline of the **key people responsible** for developing our Online-safety Policy and keeping everyone safe with ICT. It also outlines the core responsibilities of **all users** of ICT in our school.

It goes on to explain **how we maintain our policy** and then to outline **how we try to remain safe while using different aspects of ICT**

A.1 Responsibilities: online-safety coordinator

Our online-safety coordinator is the person responsible to the head teacher and governors for the day to day issues relating to online-safety. The online-safety coordinator:

- takes day to day responsibility for online-safety issues and has a leading role in establishing and reviewing the school online-safety policies and documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online-safety incident
- provides training and advice for staff
- liaises with school ICT technical staff
- receives reports of online-safety incidents and creates a log of incidents to inform future online-safety developments weekly.
- reviews weekly the output from monitoring software (Smoothwall Safeguard) and initiates action where necessary
- Liaises regularly with the online-safety lead
- attends relevant meetings and committees of Governing Body
- reports regularly to Senior Leadership Team
- receives appropriate training and support to fulfil their role effectively

A.3 Responsibilities: governors

Governors are responsible for the approval of this policy and for reviewing its effectiveness. This will be carried out by the governors receiving regular information about online-safety incidents and monitoring reports. A member of the governing body has taken on the role of online-safety governor which involves:

- regular meetings with the safeguarding lead with an agenda based on:
- monitoring of online-safety incident logs
- reporting to relevant Governors committee / meeting

A.4 Responsibilities: head teacher

- The head teacher is responsible for ensuring the safety (including online-safety) of all members of the school community, though the day to day responsibility for online-safety is delegated to the Online-safety Co-ordinator
- The head teacher and another member of the senior management team (DSL) will be familiar with the procedures to be followed in the event of a serious online-safety allegation being made against a member of staff, including non-teaching staff. (see flow chart on

dealing with online-safety incidents (included in section 2.6 below) and other relevant Local Authority / HR disciplinary procedures)

A.5 Responsibilities: classroom based staff

Teaching and Support Staff are responsible for ensuring that:

- They safeguard the welfare of pupils and refer child protection concerns using the proper channels: **this duty is on the individual, not the organisation or the school**.
- 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's Acceptable Use Agreement for staff (see Appendix 1)
- they report any suspected misuse or problem to the Online-safety Co-ordinator
- they undertake any digital communications with pupils (email / Virtual Learning Environment (VLE) / voice) in a fully professional manner and only using official systems (see A.3.5)
- they embed online-safety issues in the curriculum and other activities, also acknowledging the planned online-safety programme (see section C)

A.6 Responsibilities: ICT technician

The ICT Technician is responsible for ensuring that:

- the school's ICT infrastructure and data are secure and not open to misuse or malicious attack
- the school meets the online-safety technical requirements outlined in section B.2.2 of this policy (and any relevant Local Authority Online-safety Policy and guidance)
- users may only access the school's networks through a properly enforced password protection policy as outlined in the school's e-security policy
- shortcomings in the infrastructure are reported to the ICT coordinator or head teacher so that appropriate action may be taken.

A.7 Policy development, monitoring and review

This online-safety policy has been developed, reviewed and adapted by the Online-safety co-ordinator through working alongside the following stakeholders:

- Head teacher
- Assistant Head Teachers
- Teachers
- Governors

Schedule for development / monitoring / review of this policy

This online-safety policy was approved by the governing body on:	November 2022
The implementation of this online-safety policy will be monitored by the:	*Curriculum Committee*
The governing body will receive regular reports on the implementation of the online-safety policy generated by the safeguarding software, Senso (which will include anonymous details of online-safety incidents) as part of a standing agenda item with reference to safeguarding:	*Termly in HT report*
The online-safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of technology, new threats to online-safety or incidents that have taken place. The next anticipated review date will be:	*November 2022*
Should serious online-safety incidents take place, the following external persons / agencies should be informed:	*Worcestershire Children's First* *Local Authority Designated Officer* *Worcestershire Senior Adviser for Safeguarding Children in Education* *West Mercia Police*

A.11 Policy Scope

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

The Education and Inspections Act 2006 empowers head teachers, 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 out of school, but are linked to membership of the school.

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

A.8 Acceptable Use Agreements

All members of the school community are responsible for using the school ICT systems in accordance with the appropriate Acceptable Use Agreement (AUA), which they will be expected to sign before being given access to school systems.

Acceptable Use Agreements are provided in Appendix 1 of this policy for:

- Pupils
    - Key Stage 1

- Key Stage 2
- Staff (and volunteers)

A.9 Self Evaluation

Evaluation of online-safety is an ongoing process and links to other self evaluation tools used in school in particular pre Ofsted evaluations along the lines of the Self Evaluation Form (SEF).

A.10 Whole School approach and links to other policies

This policy has strong links to other school policies as follows:

Core ICT policies

Computing Policy	How Computing is used, managed, resourced and supported in our school.
Online-safety Policy	How we strive to ensure that all individuals in school stay safe while using Learning Technologies. The online-safety policy constitutes a part of the Computing policy and draws on training from 'Prevent'. The school's safeguarding lead has been trained in 'Prevent' strategies.
Computing curriculum	Key documents and associated resources directly relating to learning covering the Computing Curriculum

Other policies relating to online-safety

Anti-bullying	How the school strives to eliminate bullying – link to cyber bullying
PSHE	Online-safety has links to staying safe
Safeguarding	Safeguarding pupils electronically is an important aspect of Online-safety. ***The online-safety policy forms a part of the school's safeguarding policy***
Behaviour	Positive strategies for encouraging online-safety and sanctions for disregarding it.
Peer on Peer Abuse	How school strives to keep children safe at school and online
Use of images	**WCC guidance to support the safe and appropriate use of images in schools, academies and settings**

A.12 Illegal or inappropriate activities and related sanctions

The school believes that the activities listed below are inappropriate in a school context **(those in bold are illegal)** and that users should not engage in these activities when using school equipment or systems (in or out of school).

Users shall not visit Internet sites, make, post, download, upload, transfer data, communicate or pass on material, remarks, proposals or comments that contain or relate to:

- **child sexual abuse images (illegal - The Protection of Children Act 1978)**

- **grooming, incitement, arrangement or facilitation of sexual acts against children (illegal – Sexual Offences Act 2003)**
- **possession of extreme pornographic images (illegal – Criminal Justice and Immigration Act 2008)**
- **criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) (illegal – Public Order Act 1986)**
- pornography
- promotion of any kind of discrimination
- 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

Additionally the following activities are also considered unacceptable on ICT equipment or infrastructure provided by the school:

- Using school systems to undertake transactions pertaining to a private business
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by 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 (e.g. 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 gambling and non-educational gaming
- On-line shopping / commerce unless directly related to school business or in lunchbreaks or after school hours
- Use of social networking sites (other than in the school's learning platform or sites otherwise permitted by the school and to update school's own social media), unless in lunchbreaks or afterschool

	Refer to:					Inform:	Action:		
Pupil sanctions *The indication of possible sanctions in this table should not be regarded as absolute. They should be applied according to the context of any incident and in the light of consequences resulting from the offence.*	Class teacher	Online-safety coordinator	Refer to head teacher	Refer to Police	Refer to online-safety coordinator for action re	Parents / carers	Remove of network /	Warning	Further sanction e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	✔	✔	✔	✔	✔	✔	✔	✔	✔
Unauthorised use of non-educational sites during lessons	✔				✔				
Unauthorised use of mobile phone / digital camera / other handheld device	✔					✔	✔		
Unauthorised use of social networking / instant messaging / personal email	✔	✔			✔	✔		✔	
Unauthorised downloading or uploading of files	✔						✔	✔	
Allowing others to access school network by sharing username and passwords	✔	✔	✔		✔		✔	✔	
Attempting to access the school network, using another pupil's account	✔				✔		✔		
Attempting to access or accessing the school network, using the account of a member of staff	✔		✔		✔	✔		✔	
Corrupting or destroying the data of other users	✔		✔		✔	✔	✔	✔	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✔	✔	✔		✔	✔	✔	✔	
Saving files or posting any message or image that is regarded as offensive, harrassment or of a bullying nature	✔	✔	✔		✔	✔	✔	✔	
Continued infringements of the above, following previous warnings or sanctions	✔	✔	✔			✔	✔		✔
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✔		✔					✔	
Using proxy sites or other means to subvert the school's filtering system	✔	✔	✔		✔	✔	✔	✔	
Accidentally accessing offensive or pornographic material **and failing to report the incident**	✔	✔			✔	✔			
Deliberately accessing or trying to access offensive or pornographic material	✔	✔	✔		✔	✔	✔		✔

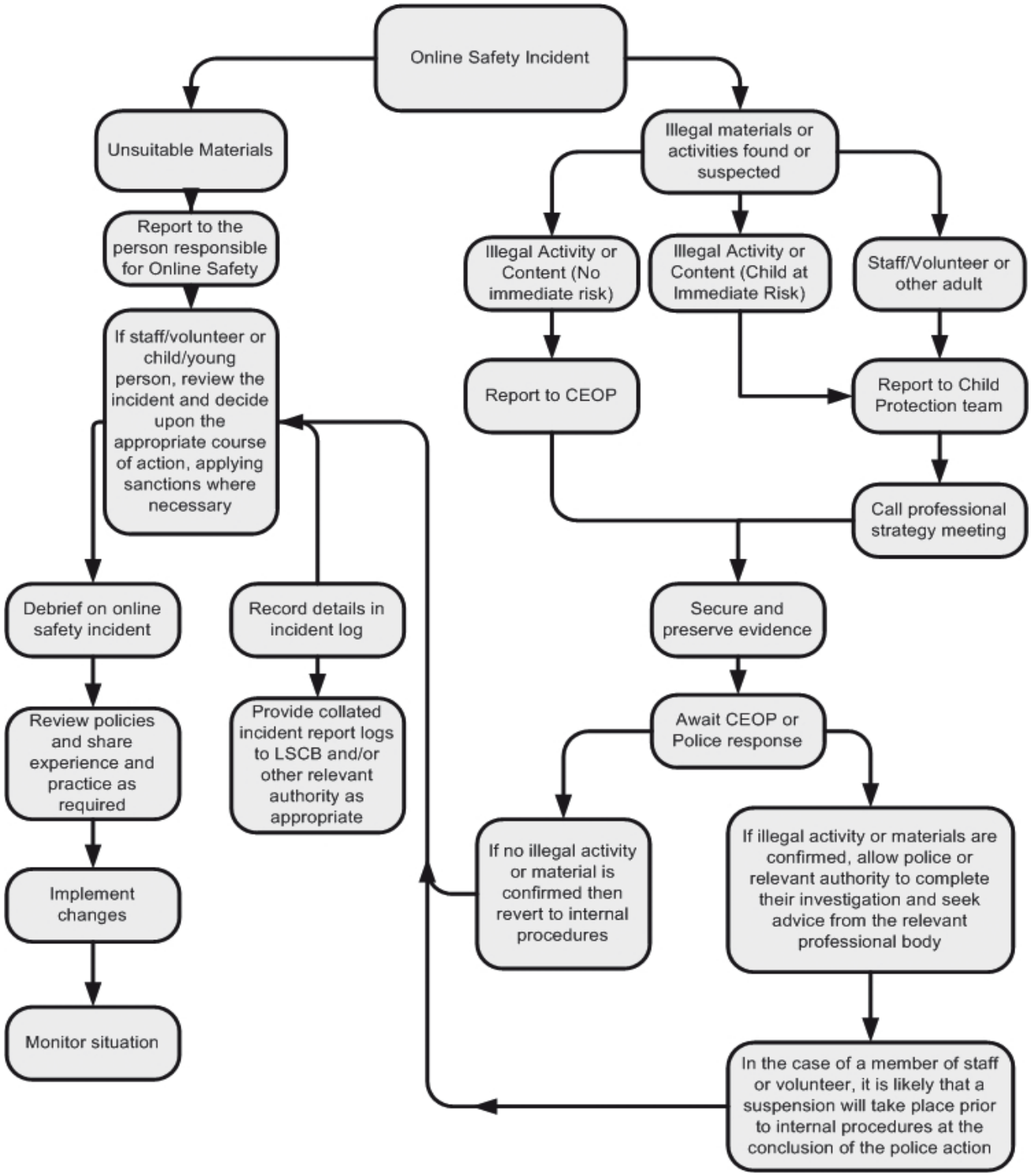
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	✔		✔		✔		✔		

	Refer to:					**Action:**		
Staff sanctions *The indication of possible sanctions in this table should not be regarded as absolute. They should be applied according to the context of any incident and in the light of consequences resulting from the offence.*	Line manager	Head teacher	Local Authority / HR	Police	Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		✔	✔	✔	✔		✔	✔
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	✔	✔				✔		
Unauthorised downloading or uploading of files	✔				✔	✔		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	✔	✔			✔	✔	✔	
Careless use of personal data e.g. holding or transferring data in an insecure manner	✔	✔	✔		✔	✔		✔
Deliberate actions to breach data protection or network security rules	✔	✔	✔		✔	✔	✔	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		✔	✔				✔	✔
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✔	✔				✔	✔	
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	✔	✔			✔			
Actions which could compromise the staff member's professional standing	✔	✔						
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✔					✔		
Using proxy sites or other means to subvert the school's filtering system	✔				✔	✔		✔
Accidentally accessing offensive or pornographic material **and failing to report the incident**	✔	✔	✔		✔	✔		

Deliberately accessing or trying to access offensive or pornographic material	✔	✔	✔		✔	✔	✔	✔
Breaching copyright or licensing regulations	✔					✔		
Continued infringements of the above, following previous warnings or sanctions	✔	✔			✔			✔

A.13 Reporting of online-safety breaches

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless, irresponsible or, very rarely, through deliberate misuse. These will be dealt with according to the disciplinary policy.


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

A.14 Use of hand held technology (personal phones and other hand held devices)

We recognise that the area of mobile technology is rapidly advancing and it is our school's policy to review its stance on such technology on a regular basis. Currently our policy is this:

- *Members of staff are permitted to bring their personal mobile devices into school. They are required to use their own professional judgement as to when it is appropriate to use them. Broadly speaking this is:*
  - ✓ *Personal hand held devices will be used in lesson time only in a school based emergency or extreme circumstances. If staff are waiting for an urgent call this must be discussed with the head teacher who will advise on the correct course of action depending on individual circumstances*
  - ✓ *Members of staff are free to use these devices outside teaching time provided they are in a private area away from children (Eg: Staff room, closed classroom, etc.)*
  - ✓ *A school mobile phone is available for professional use (for example when engaging in off-site activities). Members of staff should only use their personal device for school purposes with explicit permission from the head teacher and when withholding their number except to other school staff (eg co-ordinating times of coach arrival from several coaches)*
- *Pupils are not currently permitted to bring their personal hand held devices into school.*

	Staff / adults				**Pupils**			
Personal hand held technology *It is important that schools/academies review this table in the light of principles agreed within their own establishment.*	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff	Not allowed
Mobile phones may be brought into the school		✔						✔
Use of mobile phones in lessons				✔				✔
Use of mobile phones in social time	✔							✔
Taking photos on personal phones or other camera devices				✔				✔
Use of hand held devices e.g. iPads	✔							✔

A.14.1 - Email

These official school email services may be regarded as safe and secure and are monitored.

- Staff and pupils should use only the school email services to communicate with others regarding school business
- Users need to be aware that email communications may be monitored

- A structured education program is delivered to pupils which helps them to be aware of the dangers of and good practices associated with the use of email (see section C of this policy)
- Users must immediately report to their teacher / online-safety coordinator – in accordance with this policy (see sections A.2.6 and A.2.7) - the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature. They must not respond to any such email.

	Staff / adults				Pupils			
Use of Email *It is important that schools/academies review this table in the light of principles agreed within their own establishment.*	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff	Not allowed
Use of personal email accounts in school / on school network		✔						✔
Use of school email for personal emails				✔				✔

A.14.2 - Social networking (including chat, instant messaging, blogging etc)

No social networking is allowed during lesson time but may take place outside teaching time in a private area	Staff / adults				Pupils			
Use of social networking tools *It is important that schools/academies review this table in the light of principles agreed within their own establishment.*	Allowed	Allowed at certain times	Allowed for selected	Not allowed	Allowed	Allowed at certain times	Allowed with staff	Not allowed
Use of non educational chat rooms etc		✔						✔
Use of non educational instant messaging		✔						✔
Use of non educational social networking sites		✔						✔
Use of non educational blogs		✔						✔

A.15 Use of digital and video images

- Members of staff are allowed to take digital still and video images to support educational aims, but must follow policies concerning the sharing, distribution and publication of those images. Those images should only be captured using school equipment; **the personal equipment of staff should not be used for such purposes.**
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

- Staff should be aware of pupils for whom it has been deemed inappropriate to take and share or publish their photograph

A.16 Use of web-based publication tools

A.16.1 - Website (and other public facing communications)

Our school uses the public facing website www.millfieldsfirstschool.co.uk, ParentApps Connect (Mobile app) and a Facebook page for sharing information with the community beyond our school. This includes, from time-to-time, celebrating work and achievements of pupils. All users are required to consider good practice when publishing content.

- Personal information will not be posted and only official email addresses will be used to identify members of staff.
- Only pupil's first names will be used, and only then when necessary.
- Photographs published on the website, or elsewhere, that include pupils will be selected carefully and will comply with the following good practice guidance on the use of such images:
    - ✓ pupils' full names will not be used anywhere on a website or blog, and never in association with photographs
    - ✓ written permission from parents or carers will be obtained before photographs of pupils are published on the school website or elsewhere.

A.16.2– Learning Platform

Teachers monitor the use of our learning platform, Purple Mash, by pupils regularly during all supervised sessions, but with particular regard to messaging and communication.

Staff use is monitored by the administrator.

User accounts and access rights can only be created by the VLE administrator.

Pupils are advised on acceptable conduct and use when using the learning platform.

Only members of the current pupil, parent/carers and staff community will have access to the learning platform.

When staff, pupils, etc leave the school their account or rights to specific areas will be disabled (or transferred to their new establishment if possible / appropriate).

Any concerns with content may be recorded and dealt with in the following ways:

a) The user will be asked to remove any material deemed to be inappropriate or offensive.

b) The material will be removed by the site administrator if the user does not comply.

c) Access to the learning platform may be suspended for the user.

d) The user will need to discuss the issues with a member of SLT before reinstatement.

e) A pupil's parent/carer may be informed.

A.16.3– Accessing Learning Platform from home

When required to work from home, pupils access the learning platform following the guidelines set out above. Class teachers monitor the use of learning platforms regularly and respond through online communication via the learning platform.

Class teacher's communicating with pupils using the online learning platform will act with utmost professional standards and in line with the Computing, Online-safety and Safeguarding policies at all times. This communication will only be carried out in regards to marking or providing feedback for children's work completed from home.

The online-safety coordinator is responsible for monitoring this communication and ensuring staff are acting safely and professionally at all times.

Any concerns with content will be recorded and dealt with as described in A.16.2, following the process for reporting online-safety breaches as set out in this document.

A.16.4– Accessing Live Lessons from home

For children accessing live lessons for home (For self-isolation purposes, for example), lessons are delivered using Microsoft Teams. Each pupil have their own private account to log into their class groups, where only their peers, class teacher and headteacher can view comments or recordings. Children are encouraged to use their microphones, but keep them muted when not needed, and have the option to use their cameras if they wish.

For these live lessons, teachers deliver from appropriate locations/backgrounds. Any children in the background (If the lesson is taught from in school, for example) are included with parental permission. Lessons are recorded and saved into the class group for future access as required.

A.17 Professional standards for staff communication

In all aspects of their work in our establishment, teachers abide by the broad **Professional Standards for Teachers** laid down by the TDA effective from September 2012: http://media.education.gov.uk/assets/files/pdf/t/teachers%20standards.pdf.

Teachers translate these standards appropriately for all matters relating to online-safety.

Any digital communication between staff and pupils or parents / carers (email, chat, learning platform, etc) must be professional in tone and content.

- These communications may only take place on official (monitored) school systems.
- Personal email addresses, text messaging or public chat / social networking technology must not be used for communications with parents/ carers or pupils.

Staff constantly monitor and evaluate developing technologies, balancing risks and benefits, and consider how appropriate these are for learning and teaching. These evaluations help inform policy and develop practice. The views and experiences of pupils are used to inform this process also.

Section B. Infrastructure

B.1 Password security

The school's online-safety curriculum will include frequent discussion of issues relating to password security and staying safe in and out of school.

B.2.1 Filtering

B.2.1a - Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. No filtering system can, however, provide a 100% guarantee that it will do so.

As a school buying broadband services procured by Worcestershire County Council, we automatically receive the benefits of a managed filtering service, with some flexibility for changes at local level.

It is recognised that the school can take full responsibility for filtering on site, but current requirements do not make this something that we intend to pursue at this moment.

B.2.1b - Responsibilities

The day-to-day responsibility for the management of the school's filtering policy is held by the **online-safety coordinator** (with ultimate responsibility resting with the **head teacher and governors**).

All users have a responsibility to report immediately to teachers / online-safety coordinator any infringements of the filtering policy of which they become aware ie any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

B.2.1c – Education, training and awareness

Pupils are made aware of the importance of filtering systems through the school's online-safety education programme (see section C of this policy).

Staff users will be made aware of the filtering systems through:

- signing the Acceptable Use Agreement
- briefing in staff meetings, training days, memos etc. (timely and ongoing).

Parents will be informed of the school's filtering policy through online-safety awareness sessions / newsletter etc.

B.2.1d - Changes to the filtering system

Where a member of staff requires access to a website that is blocked for use at school, the process to unblock is as follows:

- The teacher makes the request to the school online-safety coordinator.
- The online-safety coordinator checks the website content to ensure that it is appropriate for use in school.
- If agreement is reached, the online-safety coordinator makes a request to IBS Schools Broadband Team
- The team will endeavour to unblock the site within 24 hours. This process can still take a number of hours so teaching staff are required to check websites well in advance of teaching sessions.

B.2.1e - Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the network and on school equipment.

Monitoring takes place as follows:

- Identified members of staff (members of SLT / online-safety co-ordinator / safeguarding officer) review the monitoring console captures weekly. The monitoring software is Smoothwall Safeguard
- Potential issues are referred to an appropriate person depending on the nature of the capture.
- Teachers are encouraged to identify in advance any word or phrase likely to be picked up regularly through innocent use (e.g. 'goddess' is captured frequently when a class is researching or creating presentations on the Egyptians) so that the word can be allowed for the period of the topic being taught.

B.2.2 Technical security

This is dealt with in detail in **IBS School's System and Data Security advice**. Please see that document referred to in the introduction for more information.

Section C. Education

C.1 Online-safety education

It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school approach to online safety empowers the school to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate. All staff are aware that abuse can take place solely online.

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
contact: being subjected to harmful online interaction with other users; for example: 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: online behaviour that increases the likelihood of, or causes, harm; for example, 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.
Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online-safety is therefore an essential part of the school's online-safety provision. Children and young people need constant help and support to recognise and avoid online-safety risks and build their resilience. This is particularly important for helping them to stay safe out of school where technical support and filtering may not be available to them.
Online-safety education will be provided in the following ways and will encompass the four areas of risk; content, conduct, content, commerce:

- The school uses a specific planned Online-safety curriculum.
- A planned online-safety programme is provided as part of Computing, PHSE and other lessons. This is regularly revisited, covering the use of ICT and new technologies both in school and beyond school
- Key online-safety messages will be reinforced through further input via assemblies and pastoral activities, as well as informal conversations when the opportunity arises.
- Pupils will be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use of ICT both within and outside the school.
- Processes should be in place, and known to pupils, for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit, encouraging pupils to discuss anything of which they are unsure and implementing the expected sanctions and/or support as necessary.
- Pupils will be made aware of what to do should they experience anything, while on the Internet, which makes them feel uncomfortable.

C.1.2 Information literacy

- KS2 pupils should be taught in all lessons, in an age appropriate way, to be critically aware of the content they access on-line and be guided to validate the accuracy of information by employing techniques such as:
  - ✓ Checking the likely validity of the URL (web address)
  - ✓ Cross checking references (Can they find the same information on other sites?)
  - ✓ Checking the pedigree of the compilers / owners of the website
  - ✓ Referring to other (including non-digital) sources
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils are taught how to make best use of internet search engines to arrive at the information they require
- We use the resources on CEOP's Think U Know site as a basis for our online-safety education http://www.thinkuknow.co.uk/teachers/resources/. These are mediated by a CEOP trained teacher.

C.1.3 The contribution of the pupils to the e-learning strategy

It is our general policy to encourage pupils to play a leading role in shaping the way our school operates and this is very much the case with our e-learning strategy. Pupils often use technology out of the school in ways that we do not in education and members of staff are always keen to hear of their experiences and how they feel the technology (especially rapidly developing technology such as mobile devices) could be helpful in their learning.

C.2 Staff training

It is essential that all staff – including non-teaching staff - receive online-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- An audit of the online-safety training needs of all staff will be carried out regularly.
- All new staff should receive online-safety training as part of their induction programme, ensuring that they fully understand the school online-safety policy and Acceptable Use Agreements, which are signed as part of their induction
- The Online-safety Co-ordinator (or another member of staff such as the DSL) will be CEOP trained.
- All teaching staff have been involved in the creation of this online-safety policy and are therefore aware of its content
- The Online-safety Coordinator will provide advice, guidance and training as required to individuals as required on an ongoing basis.
- External support for training, including input to parents, is sought from appropriately qualified persons when required.

C.3 Governor training

Governors should take part in annual online-safety training with particular importance for those who are members of any subcommittee or group involved in ICT, online-safety, health and safety or child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority (Governor Services or School Improvement Service), National Governors Association or other bodies.
- Participation in school training / information sessions for staff or parents

The online-safety governor works closely with the DSL and reports back to the full governing body.

C.4 Parent and carer awareness raising

Some parents and carers have a limited understanding of online-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of their on-line experiences. Some parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it.

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site
- Parents evenings

Millfields First School

KS1 Acceptable User Agreement

This is how we stay safe when we use technology at school and home:

- I will ask an adult if I want to use a computer or iPad.
- I will only use activities if an adult says it is ok.
- I will take care of the computer and other equipment.
- I will keep my passwords safe and private.
- I will only post friendly and kind messages online.
- I will ask for help from an adult if I am not sure what to do or if I think I have done something wrong
- I will turn off the monitor and tell an 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.

I understand these computing rules and will do my best to keep them

Class:	
Signed (children):	
Date:	

Millfields First School

KS2 Acceptable User Agreement

Acceptable Use Agreement – Key Stage Two- for school and school work at home

I understand that I must use technology in a responsible way.

For my own personal safety:

- I understand that my use of technology (especially when I use the internet) will be supervised in school.
- I will keep my password safe and private, and I will not use anyone else's (even with their permission).
- I will keep my own personal information safe, as well as others.
- I will tell a trusted adult if anything makes me uncomfortable or upset when I see it online.

For the safety of others:

- I will not interfere with the way that others use technology.
- I will be polite and responsible when I communicate with others; I will not post anything that is not kind about anyone.
- I will not take or share images of anyone without their permission.

For the safety of the school:

- I will not try to access anything illegal.
- I will not download anything that I do not have the right to use.
- I will only use my own personal device if I have permission and use it within the agreed rules.
- I will not deliberately bypass any systems designed to keep the school/academy safe.
- I will tell a responsible person if I find any damage or faults with technology, however this may have happened.
- I will not attempt to install programmes of any type on devices belonging to the school without permission.
- I will only use social networking, gaming and chat through the sites the school allows.

I understand that I am responsible for my actions and the consequences. I have read and understood the above and agree to follow these guidelines:

Class:	
Signed (children):	
Date:	

Staff (and Volunteer) – Acceptable Use Agreement

Acceptable Use Agreement – Staff (and Volunteers)

By signing this agreement, you will have access to the school's systems and acknowledge that you agree to all the statements below. Additionally, that you have read and understand school policies which have a bearing on this agreement (Computing, Online-safety and Safeguarding policies).

- I will demonstrate the value of the use of digital technologies in improving the outcomes for children in my care.
- I will educate children in my care about the safe use of digital technologies, acting on any online safety issues in accordance with the school's policies.
- I understand my use of the school's ICT systems/networks and internet are monitored.
- I recognise that whether within school or out of school, I must abide by the rules/statements set out in this document when using systems, accessing/transferring data that relate to the school or impact on my role within the school and wider community.
- I know what GDPR is and how this has a bearing on how I access, share, store and create data.
- Any data that I have access to away from school premises must be kept secure and used with specific purpose. As outlined in the school's data protection policy, it is my responsibility to ensure when accessing data remotely that I take every bit of reasonable care to ensure the integrity and security of the data is maintained.
- I understand that I am fully responsible for my behaviours both in and out of school and as such recognise that my digital communications, subscriptions and content I access can have a bearing on my professional role.
- I recognise that my social media activity can have a damaging impact on the school and children in my care at school if I fail to uphold my professional integrity at all times whilst using it.
- If I am contributing to the school's social media account(s) or website(s) I will follow all guidelines given to me, with particular care given to what
- I will never upload images/video imagery of staff/pupils or other stakeholders to my personal social media accounts unless there is significant reason to and that explicit permission has been granted by the headteacher in writing for each occurrence.
- I will inform the school at the earliest opportunity of any infringement both on and off site by myself. Furthermore, if I am concerned about others' behaviour/conduct, I will notify the school at the earliest opportunity.
- I will never deliberately access, upload or download illegal, inflammatory, obscene or inappropriate content that may cause harm or upset to others.
- I will never download or install software unless permission has been given by the appropriate contact at school.
- I shall keep all usernames and passwords safe and never share them
- I will never leave equipment unattended which could leave data and information vulnerable; this extends to accessing data/services/content remotely.
- I will always lock my screen when leaving my computer.
- Any personal devices I own shall not be used to access school systems/data/services/content remotely unless I have adequate virus protection and permission from the school.
- I understand that mobile devices shall not be used, during times of contact with children. These devices will have adequate password protection on them should they be accessed by an unauthorised person.
- At no point- will I use my own devices for capturing images/video of our school children
- If I need to use my own phone for making calls to parents (with specific permission from the head teacher) I will make sure that my number is withheld

images/video imagery and details can be uploaded.

- If I am meeting with parents or teaching via an online programme from home (e.g. Teams/Zoom), I will make sure that my background is blurred or a different one added so that my home is not visible to parents/ children
- I will not use USB/ pen drive for transferring/ storing information

Name	
Role	
Signature	
Date	