On-line Safety

Document Control Information

Version	DATE	DESCRIPTION
1	18/11/2020	
2	1.11.2021	
3	1.11.2022	Some amendments updated KCSIE 2022
4	14.02.24	

Reviewed	1.11.22
Responsibility	Sian Vaux
Committee	FGB
Review Date	11/2024
Signed	Siân Vaux

CONTENTS

Section	Title	Page
1	Online Safety Statement	3
2	Key Personnel	3
3	Terminology	4
4	Introduction	5
5	Policy Aims	6
6	Statement of Policy Intent	6
7	Policy Scope	6
8	Roles and Responsibilities	6-8
9	Policy Development, Monitoring and Review	9
10	Acceptable Use Policies	9
11	Self Evaluation	9
12	Illegal or Inappropriate Activities and Related Sanctions	10
13	Audit, Monitoring, Reporting and Review	13-15
14	Filtering	15
15	Education, Training and awareness	16-18
16	Equality and Inclusion	18

Annexes:

A	Online Safety Incident Flowchart
B	Acceptable Use Policy - Pupils (EYFS + KS1 / KS2)
C	Acceptable Use Policy – Staff and Volunteers
D	Acceptable Use Policy and Permissions Form Parents/Carers
E	Acceptable Use Policy – Community User
F	Guidance for Reviewing Websites
G	Criteria for Website Filtering

1. ONLINE SAFETY MISSION STATEMENT

1.1 Meath School will abide by the following Online Safety Statement:

> Meath School works to create a calm supportive learning environment where high standards of behaviour and conduct on-line are expected from all members of the school community.

2. KEY PERSONNEL

2.1 The Online Safety Officer is: Majella Delaney, Principal
Contact details: email: Majella.delaney@meathschool.org.uk
telephone: 01932 872302

2.3 The Principal is: Majella Delaney
Contact details: email: as above
telephone: 01932 872302

2.4 The Chair of the SAB is: Sian John
Contact details: email: sian.john@meathschool.org.uk

3. TERMINOLOGY

Online Safety is defined as:

- The safe and responsible use of technology
- Protecting and educating pupils and staff in their use of technology
- Having the appropriate mechanisms to intervene and support any incident, where appropriate

Child(ren) includes everyone under the age of 18. This will apply to pupils attending our school. The policy will extend to visiting children and students from other establishments

CEOP refers to Child Exploitation and Online Protection Command

Closed Social Media refers to social media that can only be shared to a limited number of selected people

DSL and DDSL refers to Designated Safeguarding Lead and Deputy Designated Safeguarding Lead

Digital Literacy refers to the ability to find, evaluate, use, share and create content using IT and the internet

GDPR refers to General Data Protection Regulation

Governor's Safeguarding, Behaviour and Welfare Committee refers to the committee run by the Governing Body to provide oversight and guidance in respect of Health and Safety to Meath School

Meath, a Speech and Language, UK School refer to all members of Staff, the Governors and Volunteers who are associated with the school

Meath School Online Safety Committee refers to the team that meet to ensure online safety is up to date and relevant at Meath School

Parents refers to birth parents and other adults who are in a parenting role, for example stepparents, foster carers and adoptive parents

Staff refers to all those working for or on behalf of the school, full or part time, temporary or permanent, in either a paid or voluntary capacity

SSCP refers to the Surrey Safeguarding Children Partnership

VLE refers to Virtual Learning Environment or a web-based platform for study, e.g. Seesaw

4. INTRODUCTION

4.1 Current legislation requires Meath School to produce a written statement outlining its Online Safety philosophy. In consequence, this Online Safety policy has been drawn up to meet the legal requirements which are binding on employer and employee alike. This Meath School Online Safety document forms part of Speech and Language UK's Online Safety Policy.

4.2 This policy document builds on what is considered to be the best and most effective Online Safety practice and provides a formal structure within which this practice may be implemented consistently and fairly. It is designed to ensure consistency of application in encouraging respect for others, rewarding positive attitudes, good behaviour and a positive environment for everyone.

4.3 The pupils at Meath School present with severe and complex speech, language and communication needs (including high functioning autistic learners) that affect, to varying extents, their ability to understand and use language effectively for all communication. This can affect their understanding of the correct way of communicating and the meaning of communication.

4.4 It is essential that Staff appreciate the difficulties a pupil may have in understanding what is expected of them and coping with the frustrations of their communicative needs. We must recognise the communicative importance of all behaviour whether they conform or not. It means that it is difficult for our pupils to understand that other people would want to cause them harm or not be telling the truth which can make them extremely vulnerable.

4.5 **Online Risks**. The potential that technology has, to impact on the lives of all citizens increases year on year. Children are generally more open to developing technologies than many adults. In many areas, technology is transforming the way that schools teach, and children learn. At home, technology is changing the way children live and the activities in which they choose to partake. These trends are set to continue.

4.6 While developing technology brings many opportunities, it also brings risks and potential dangers including:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact 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 use which may impact on social and emotional development and learning

4.7 Meath School's Online Safety Policy has been written taking into account Surrey County Council (SCC) Online Safety Guidelines. https://www.healthysurrey.org.uk/professionals/healthy-schools/news/teaching-online-safety-in-schools and https://www.surreycc.gov.uk/children/support-and-advice/families/support-and-advice/keeping-your-family-safe/internet-safety

4.8 **Statutory Requirements and Guidance**. This Meath School Online Safety policy has been developed in accordance with the relevant provisions of the Children Act (1989); Keeping Children Safe in education (updated 2022); Computer Misuse Act (1990); Criminal Justice and Immigration Act (2008); Education Act (1996); Education Act (2011) Part 2 (Discipline); Education and Inspections Act (2006); Data Protection Act (2018); Health and Safety at Work etc. Act (1974); Human Rights Act (1998); Protection of Children Act (1978); Sexual Offences Act (2003); Public Order Act (1986); Obscene Publications Act (1959) and the School Behaviour (Determination and Publicising of Measures in Academies) Regulations 2012.

4.9

KCSIE 2023

- Specific online safety content has been added and strengthened in part two to ensure online safety is viewed as part of a school/college's statutory safeguarding responsibilities.
- Part two now signposts DSLs and school/college leaders to the DfE 'Harmful online challenges and online hoaxes' guidance.
- All School Advisory Board Members and trustees should receive appropriate online safety information/training as part of their safeguarding and child protection training; this should be received as part of their induction and be regularly updated.
- School Advisory Board Members/trustees should ensure that the school/college leadership team and relevant staff have an awareness and understanding of the appropriate filtering and monitoring provisions in place, manage them effectively and know how to escalate concerns when identified.
- New content has been added to part two to recognise the importance of schools/colleges communicating regularly with parents to reinforce the importance of children being safe online.

5. POLICY AIMS

5.1 The aim of this Online Safety Policy is to:

- Identify the legislation and other statutory guidance affecting Meath School's Online Safety
- Identify the roles and responsibilities of members of the Meath School Staff and Governing Body
- State the Speech and Language, UK / Meath School procedures for incidents concerning Online Safety
- Link its provisions, including the roles and responsibilities and acceptable actions and sanctions to other relevant Meath School policies listed on the front cover

6. STATEMENT OF POLICY INTENT

6.1. This policy sets out how Meath School will strive to keep children safe with technology while they are in school. Staff recognise that children are often more at risk when using technology at home (where the school has no control over the technical structures designed to keep them safe) and so this policy also sets out how we educate children of the potential risks.

6.2 The policy explains how the school will attempt to inform those people who work with our children beyond the school environment (parents/carers, friends and the wider community) to be aware and to assist in this process.

6.3 Meath School will ensure that it takes all measures necessary to rectify any fault or problem that occurs giving rise to an Online Safety issue.

7. POLICY SCOPE

7.1 This policy applies to all members of the school community (including Staff, pupils, volunteers, parents / carers, Governors, visitors, community users) who have access to and are users of school IT systems, both in and out of school.

7.2 The Education and Inspections Act (2006) empowers Principals, 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 is linked to membership of the school.

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

8. ROLES AND RESPONSIBILITIES

8.1 **Principal**. The Principal is responsible for ensuring the safety including Online Safety of all members of the school community. Day to day responsibility for Online Safety is delegated to the Designated Safeguarding lead and the Online Safety Committee.

8.2 The Principal and all members of the Senior Leadership Group (SLG) are to be aware of the procedures to be followed in the event of a serious Online Safety allegation being made against a member of Staff (**see Annex A, the Online Safety incidents flowchart**). The SLG is to be familiar with all relevant HR disciplinary procedures.

8.3 **Online Safety Committee**. The Meath School Online Safety Committee is delegated by the DSL and Principal to lead on all matters relating to Online Safety and report to the Governing body.

8.4 The Committee is led by the Online Safety Manager (Principal) and comprises the Residential Services Manager, the Safeguarding and Pastoral Lead, the curriculum lead for Computing and the Online Safety Governor.

8.5 The Committee meets on a termly basis to:

- Review and monitor this Online Safety policy, updating it as required (annual audit of online safety)
- Consider any issues relating to Meath School (internet) filtering working with SENSO and Bluecube.
- Discuss any Online Safety issues that have arisen since the last Committee meeting and how they should be dealt with.

8.6 Serious issues arising may be referred to the Surrey Safeguarding Children Board (SSCP). using this link Referral procedure

8.7 **Online Safety Manager (Principal)**. The Online Safety Manager reports to the DSL, and Governors in respect of day-to-day issues relating to Online Safety and is responsible for:

- Chairing the Meath School Online Safety Committee meetings

- Attending relevant meetings and committees of the Governing Body Informing the Governors of Online Safety incidents and reports
- Reporting weekly to SLG
- Is to be CEOP (or equivalent) and DSL trained
- Reviewing and updating the Online Safety Policy and associated documents
- Ensuring that Staff are aware of the procedures that need to be followed in the event of an Online Safety incident
- Providing training and advice for Staff
- Liaising with school IT technical staff (Bluecube)
- Monitoring reports of Online Safety incidents on CPOMS to inform future Online Safety developments and training
- Meeting with the Online Safety Committee to discuss current issues, review incident logs and filtering change control logs

8.8 **Business Manager**. The Meath School Business manager is to:

- Maintain and update a record of all Staff, volunteers, pupils, Governors and visitors who are granted access to use any Meath School IT
- Maintain a central register of all IT training (the Single Central Record)
- Support the Premises Manager in all matters relating to the contracting for IT hardware, software, training and support, maintaining records as appropriate

8.9 **Governing Body**. The Meath School Governing Body is responsible for:

- Approving this policy
- Designating a member to take on the role of Online Safety Governor
- Termly meetings with the Online Safety Manager to:
    - Review Online Safety logs
    - Monitor filtering change control logs

- Review any search and deletion logs

8.10 **Classroom Staff**. The teaching and support Staff are responsible for ensuring that:

- They have an up-to-date awareness of Online Safety matters and of the current Meath School Online Safety policy and practices
- They have read, understood and signed the school's Acceptable Use Policy for Staff
- They report any suspected misuse or problem to the Online Safety Manager and recorded it on CPOMS under the category Online Safety
- Digital communications with students (email / social media software /voice) should be on a professional level and only carried out using official school systems
- Online Safety issues are embedded in the curriculum and other school activities

8.11 **IT Technician (Bluecube)**. The IT Technician is responsible for ensuring:

- The school's IT infrastructure is secure and is not open to misuse or malicious attack, security will be reviewed by the Online Safety Committee termly and/or in the event of serious attack
- That users may only access the school's networks through properly enforced password protection
- Shortcomings in the infrastructure are reported to the Computing Coordinator or Principal so that appropriate action may be taken
- All internet access has age-appropriate filtering provided by a recognised filtering system which has been checked to ensure that it is working, effective and reasonable
- Internet sites deemed by the school to be inappropriate are blocked by the school's filtering system
- That Meath School uses a recognised internet provider
- That the Meath School network is protected with appropriate anti-virus software

9. POLICY DEVELOMENT, MONITORING AND REVIEW

9.1 **Schedule for Development, Monitoring and Review**. This policy will be monitored and reviewed as follows:

Monitoring of the provisions in the policy by the Committee	Continuous
Drafting of amendments by the Committee following changes in statute and/or guidance	Continuous
Verbal Online Safety report produced by the Committee for the SAB	Termly
Full review by the Committee (audit)	Autumn Term each year
In the event of a serious Online Safety incident the Online Safety Manager is to inform:	• SSCP Online Safety representative • Surrey Police • CEOPS

10 ACCEPTABLE USE POLICIES

10.1 All members of the Meath School community are responsible for using the school IT systems in accordance with their respective Acceptable Use policy, which they are to read and sign before being granted access.

10.2 The school Acceptable Use policies are at Annexes B to E:

- Pupils (EYFS + KS1 / KS2)
- Staff and volunteers
- Parents / carers agreement for their child/ren to use IT systems
- Community users of the school's IT system

10.3 The policies can change in the light of new developments and discussions with Staff and/or children or as the result of changes to statute and/or official guidance. Copies of the policies for the children are to be sent home for parents/carers.

10.4 For children in EYFS and KS1 parents/carers may sign on behalf of their children. Staff and volunteers sign when they take up their role in school and on an annual basis. A record of signatures is to be kept as part of the school Single Central Record held by the Business Manager.

10.5 Parents/carers sign once when their child enters the school. The parents' policy includes permission for their child to use the School's IT resources (including the internet) and permission to publish their work. A copy of the Pupil Acceptable Use policy is made available to parents/carers at this stage and at the beginning of each year.

10.6 Community users are to sign the Community User Acceptable Use policy when they first request access to the school's IT system.

10.7 Induction policies for all members of the school community are to include this guidance.

11. SELF EVALUATION

11.1 Evaluation of Online Safety is an on-going process and links to other self-evaluation tools used by Meath School. In particular to pre-Ofsted evaluations along the lines of the Self Evaluation Form (SEF). The views and opinions of all stakeholders (pupils, parent/carers, teachers) are taken into account as a part of this process.

12. ILLEGAL OR INAPPROPRIATE ACTIVITIES AND RELATED SANCTIONS

12.1 Meath 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, data transfer, 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)**
- **The 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) (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

12.3 Additionally the following activities are also considered unacceptable on Meath School IT:

- Using school systems to run a private business
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Speech and Language, UK and / or Meath 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, including 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

12.4 If members of Staff suspect that misuse might have taken place, but that the misuse is not illegal (see above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. Staff are to check the tables below and inform the appropriate authority. See also **Annex F in respect of Guidance for Reviewing Internet Sites.**

12.5 It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. Incidents are to be dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

12.6 **Pupil Sanctions**.

	Refer to class teacher	Refer to Online Safety Manage	Refer to Principal	Refer to Police	Refer to Online Safety Manager	Inform parents / carers	Removal of network / internet access	Warning	Further sanctions detention /
Deliberately accessing or trying to access material that could be considered illegal (see list of unsuitable / inappropriate activities)	✓	✓	✓		✓	✓	✓	✓	✓
Unauthorised use of non-educational sites during lessons	✓				✓		✓		
Unauthorised use of mobile phone / digital camera / another 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	✓	✓	✓			✓		✓	

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	✓	✓	✓		✓	✓	✓	✓	

12.7 **Staff Sanctions**.

	Refer to line manager	Refer to Principal	Refer to Police	Refer to 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 above 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 eg 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 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	✓	✓			✓	✓	✓

12.8 It is anticipated that all members of the school community will be responsible users of IT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

13. AUDIT, MONITORING, REPORTING AND REVIEW

13.1 The Online Safety Manager will ensure that full records are kept of incidents involving the searching for and of mobile phones and electronic devices and the deletion of data / files on CPOMS.

13.2 These records will be reviewed by the DSL and Principal and on a termly basis.

13.3 **Use of Handheld Technology - Personal Telephones and Hand-Held Devices**. Meath School recognises that the area of mobile technology is rapidly advancing, and it is the school's policy to review its stance on such technology on a regular basis. Currently our policy is this:

13.4 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 handheld devices will be used in lesson time only in an emergency or extreme circumstances

- Members of Staff are free to use these devices in school, outside teaching time (away from the children)

- Pupils who bring their personal handheld devices into school – class staff ensure these devices are locked away and returned to the child for their journey home.

13.5 **Email**. Access to email is provided for all users in school. The Meath 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 when in school, or on school systems (e.g. by remote access)

- Users need to be aware that email communications may be monitored

- Pupils have access to an individual email account for communication within school

- A structured education programme is delivered to pupils which help them to be aware of the dangers of and good practices associated with the use of email

- Staff may only access personal email accounts outside of child contact time

13.6 Users must report immediately their class teacher / Online Safety Manager – in accordance with the school policy the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

13.7 Incoming email from an unknown source must be treated as suspicious and attachments not opened.

13.8 **Video Conferencing**. Video Conferencing equipment is used in the Residential Department and must be switched off when not in use and not set to auto answer.

13.9 Meath School external IP addresses are not to be made available to other sites/users.

13.10 The Video Conferencing contact information is not to be published on the school website.

13.11 Only web-based conferencing products that are authorised by the school are permitted for classroom use.

13.12 Video Conferencing is to be supervised by a member of Staff. In the event of this not being the case pupils should ask permission from the supervising member of Staff before making or answering a Video Conference call.

13.13 Permission for children to take part in Video Conferences is sought from parents /

carers at the beginning of the pupil's time in schools and only where it is granted may children participate.

13.14 Only key IT administrators are to have access to Video Conferencing administration areas.

13.15 **Use of Digital and Video Images**. Staff are to inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should identify the risks attached to publishing their own images on social networking sites.

13.16 Members of Staff are allowed to take digital still and video images to support educational aims, but must follow Meath School policies concerning the sharing, distribution and publication of those images. Those images should only be captured using school equipment; the personal equipment of Staff are not to be used for such purposes. In particular, devices are to be checked regularly to ensure that web-based back-up Apps and programmes for example, iCloud, have not been switched on during software upgrades.

13.17 Care should be taken when taking digital / video images that pupils are appropriately dressed.

13.18 Pupils must not take, use, share, publish or distribute images of others without their permission.

13.19 **Use of Web-Based Publication Tools**. Meath School uses the public facing website, www.meathschool.org.uk for sharing information with the community beyond the school. This includes, from time-to-time celebrating work and achievements of children. All users are required to consider good practice when publishing content.

13.20 Personal information is not to be posted on the school website and only official email addresses (provided as links rather than appearing directly on the site) should be used to identify members of staff (never pupils).

13.21 Only pupil's first names are used on the website, and only then when necessary.

13.22 Detailed calendars are not published on the school website.

13.23 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

- Annual written permission from parents or carers will be obtained before photographs of pupils are published on the school website

- Pupil's work can only be published with the permission of the pupil and parents / carers

13.24 **Digital Literacy and Closed social media**. Class teachers are to monitor the use of closed social media by pupils regularly in all areas, but with particular regard to messaging and communication.

13.25 Staff use is monitored by the administrator.

13.26 User accounts and access rights can only be created by the school administrator and the IT technician.

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

13.28 Only members of the current pupil, parent/carers and Staff community will have access to a closed social media or email tool.

13.29 When Staff, volunteers, Governors and pupils leave the school, their account or rights to specific school areas will be disabled or transferred to their new establishment if possible / appropriate.

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

- The user will be asked to remove any material deemed to be inappropriate or offensive

- The material will be removed by the site administrator if the user does not comply

- Access to closed social medial for the user may be suspended

- The user will need to discuss the issues with a member of SLG before reinstatement

- A pupil's parent/carer may be informed.

- It will be reported on CPOMS

13.31 A visitor may be invited onto closed social by the administrator (usually the computing Coordinator) following a request from a member of Staff. In this instance there may be an agreed focus or a limited time slot / access.

13.32 **Professional Standards for Staff Communication**. In all aspects of their work in our school, teachers abide by the Teachers' Standards as described by the DfE (Teaching standards). Teachers are to translate these standards appropriately for all matters

relating to Online Safety.

13.33 Any digital communication between Staff and pupils or parents / carers (email, chat, VLE) 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 these communications.

13.34 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.

14. FILTERING

14.1 **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. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

14.2 **Responsibilities**. The day-to-day responsibility for the management of the school's filtering policy is held by the IT Company (ultimate responsibility rests with the Principal). The IT Company is to manage the school filtering, in line with the processes outlined below and keep logs of changes to and breaches of the filtering system (see Annex F in respect of Criteria for Website Filtering).

14.3 To ensure that there is a system of checks and balances and to protect those responsible the school will:

- be informed of any safeguarding tickets raised by the school with the IT Company

- be made aware prior to changes being made (this will normally happen anyway, as part of the process and will be the Online Safety Manager).

14.4 All users have a responsibility to report immediately to class teachers / Online Safety Manager/Business Manager any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should be blocked.

14.5 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.

15. EDUCATION, TRAINING AND AWARENESS

15.1 Pupils are made aware of the importance of filtering systems through the school's

Online Safety education programme.

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

- Signing the AUP as part of their induction process

- Briefings during Staff meetings, training days and periodic update memos

15.3 Parents/carers will be informed of the school's filtering policy through the Acceptable Use Agreement and through Online Safety awareness sessions / newsletter / drip feeding and online safety workshops / bulletins etc.

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

15.5 **Audit / Reporting**. Logs of filtering change controls and of filtering incidents are made available to:

- The Online Safety Governor
- The Online Safety Committee

15.6 The filtering log will be reviewed in response to the evidence provided by the audit logs of the suitability of the current provision.

15.7 **Online Safety Education**. Whilst regulation and technical solutions are particularly 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 the help and support of the school to recognise and avoid Online Safety risks and build their resilience. This is particularly important for helping children to stay safe out of school where technical support and filtering may not be available to them.

15.8 Online Safety education will be provided in the following ways:

- A planned Online Safety programme will be provided as part of Computing, PHSE and other lessons. It will be regularly revisited and will cover both the use of IT and new technologies in school and outside school

- Meath School uses the resources on **CEOP's Think U Know site** as a basis for Online Safety education https://www.thinkuknow.co.uk/ (Hector's World at KS1 and Cyber Café at KS2)

- Key Online Safety messages are to be reinforced through further input via assemblies and pastoral activities as well as informal conversations when the opportunity arises as well as through safer internet day activities

- Pupils are to be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of IT both within and outside school

15.9 In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

15.10 Where pupils are allowed to freely search the internet including using search engines, Staff should be vigilant in monitoring the content of the websites the young people visit. This can be facilitated using Kids Search.

15.11 **Information Literacy**. Pupils will be taught in all lessons 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
- See Lesson 5 of the Cyber Café Think U Know materials below
- Pupils are to be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils are to be taught how to make best use of internet search engines to arrive at the information they require

15.12 **The Contribution of the Children to the Online Learning Strategy**. It is our general school policy to require children to play a leading role in shaping the way our school operates and this is very much the case with our Online Learning Strategy. Children often use technology out of school in ways that we do not in school and members of Staff are always keen to hear of children's experiences and how they feel the technology, especially rapidly developing technology (such as mobile devices) could be helpful in their learning.

15.13 Pupils play a part in contributing to this policy through the School Council.

15.14 **Staff Training**. It is essential that all Staff receive Online Safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal Online Safety training will be made available to Staff. An audit of the Online Safety training needs of all staff will be carried out regularly
- It is expected that some Staff will identify Online Safety as a training need within the performance management process

- All new Staff are to receive Online Safety training as part of their induction programme, ensuring that they fully understand the Meath School Online Safety policy and Acceptable Use policies which are signed as part of their induction

- The Online Safety Manager will receive regular updates through attendance at training sessions and by reviewing guidance documents released by the DfE, local authority, the SSCB and others

- All staff to complete the National Online Safety Annual training using the online platform https://nationalonlinesafety.com/

- All training completed is to be recorded by the Business manager in the Single Central Record

15.15 The Online Safety Committee will provide advice, guidance and training as required to individuals as required on an on-going basis.

15.16 **Governor Training**. All Meath School Governors are to be offered Online Safety training / awareness sessions, with particular importance for those who are members of any subcommittee or group involved in IT, Online Safety, Health and Safety or Safeguarding and Child Protection. This may be offered in a number of ways:

- Attendance at training offered by an approved external provider

- Participation in school training / information sessions for Staff or parents/carers

- Completion of the National Online Safety Annual training for Governors using the online platform https://nationalonlinesafety.com/

15.17 The Online Safety Manager is to work closely with the Online Safety Governor and reports back to the Online Safety Committee. The Online Safety Governor is to report back to the Governing Body on a termly basis.

15.19 **Parent / Carer Awareness Raising**. Many parents and carers have only 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 the children's on-line experiences. Parents/carers 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. "There is a generational digital divide". (Byron Report).

15.20 Meath School will seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site, VLE

- Parents evenings
- Reference to the parents' materials on the Think U Know website (www.thinkuknow.co.uk) or others
- Drip feeding of information relating to areas of interest of children and their siblings.
- Online safety workshops and bulletins at whole school events.

15.21 **Wider School Community Understanding**. The school will offer family training in IT, media literacy and Online Safety so that parents/carers and children can together gain a better understanding of these issues. Messages to the public around Online Safety should also be targeted towards grandparents and other relatives as well as parents/carers. Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

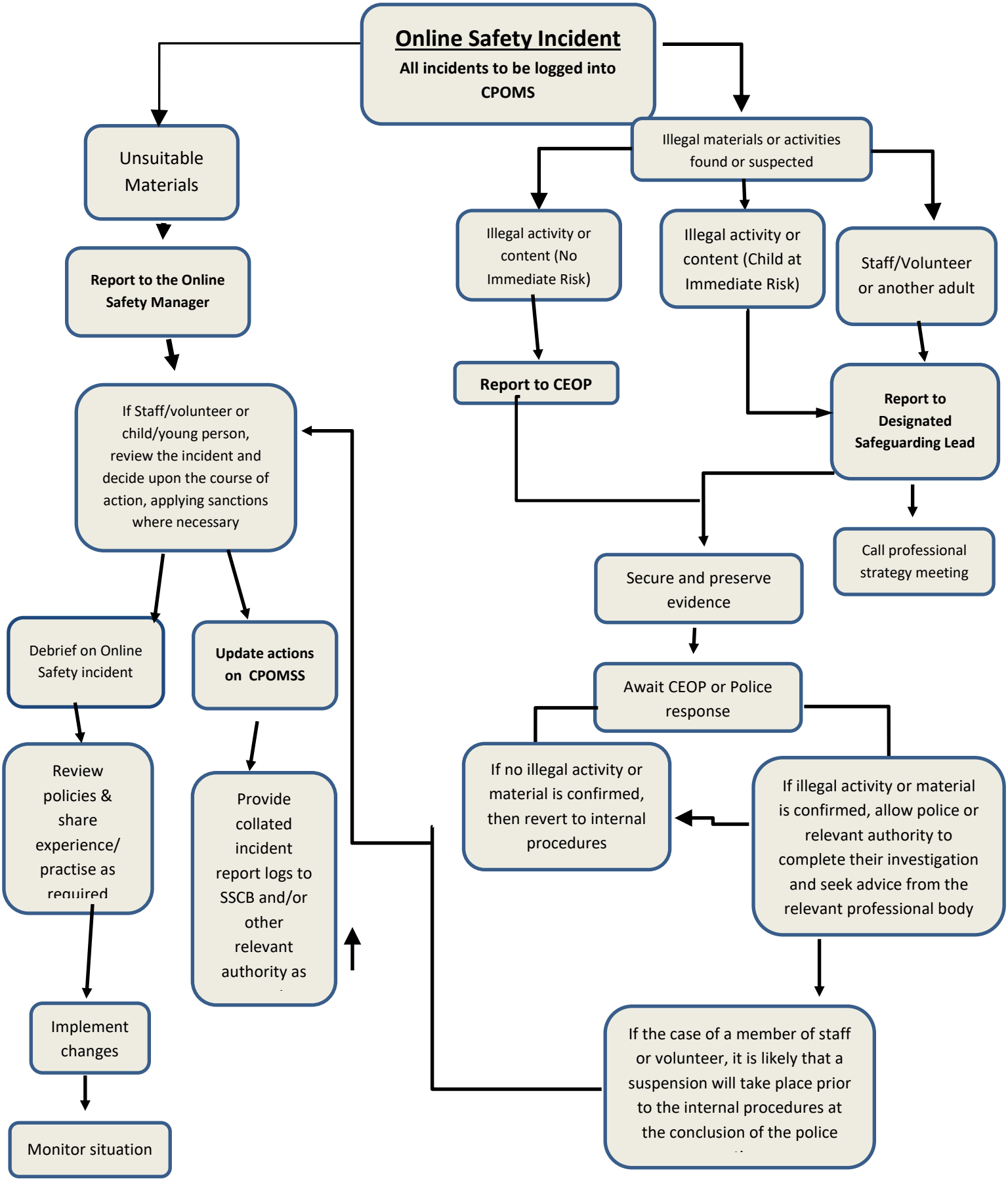
15.22 Community Users who access school IT systems / website / VLE as part of the Extended School provision will be expected to sign a Community User AUP before being provided with access to school systems.

16. EQUALITY AND INCLUSION

16.1 Meath School will continuously seek to ensure that all members of the school community are treated with respect and dignity. Every individual will be given fair and equal opportunities to develop their full potential regardless of their gender, ethnicity, cultural and religious background, sexuality, disability or special educational needs and ability, and other factors as detailed within the school's Equality Policy. These meet in full the requirements of the Equality Act (2010).

ANNEX A TO ONLINE SAFETY POLICY

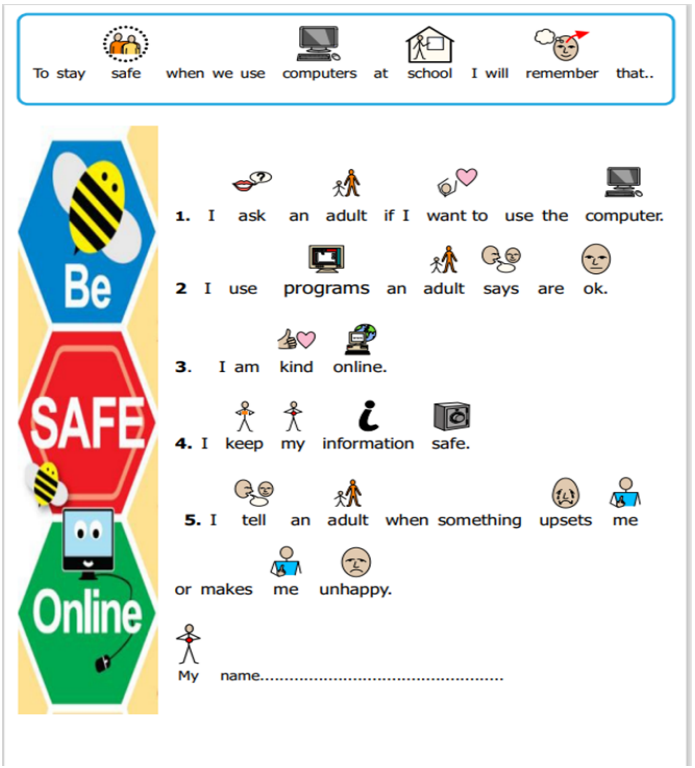
ONLINE SAFETY INCIDENT FLOWCHART

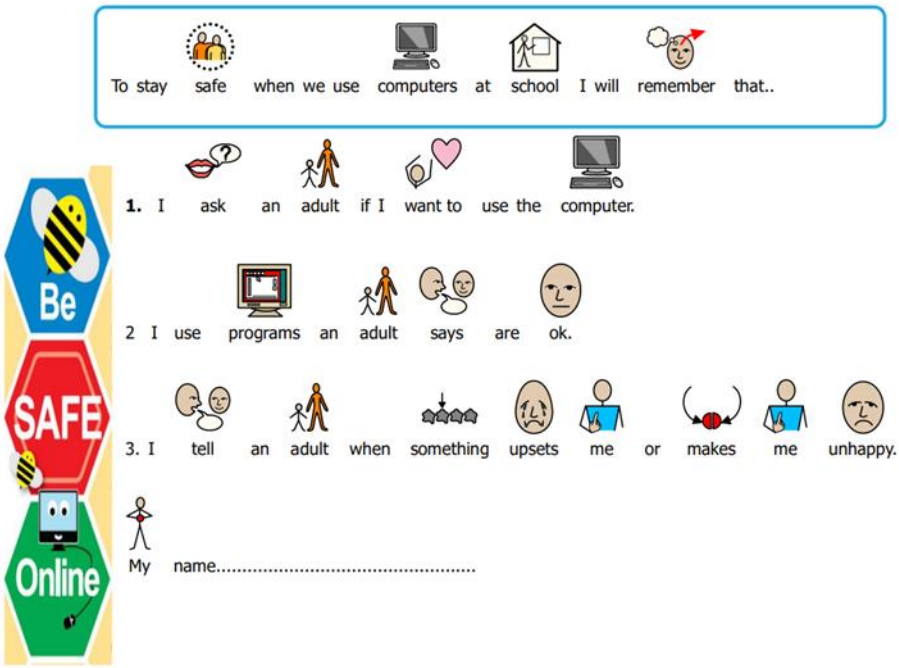


ANNEX B TO ONLINE SAFETY POLICY

MEATH SCHOOL

ACCEPTABLE USER POLICY AGREEMENT – PUPILS (EYFS + KS1/KS2)





ANNEX C TO ONLINE SAFETY POLICY

MEATH SCHOOL

ACCEPTABLE USER POLICY AGREEMENT – STAFF AND VOLUNTEER

1. BACKGOUND

1.1 Technology has transformed learning, entertainment, and communication for individuals and for all organisations that work with young people. However, the use of technology can also bring risks. All users should always have an entitlement to safe internet access.

1.2 I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I will, where possible, educate the young people in my care in the safe use of ICT and embed Online Safety in my work with young people.

1.3. **For my professional and personal safety:**

- I understand that Meath School will monitor my use of the IT systems, email and other digital communications
- I understand that the rules set out in this Agreement also apply to use of school IT systems (laptops, email, VLE etc) out of school
- I understand that the Meath School IT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set out in the Meath School Online Safety policy
- I will not disclose my username or password to anyone else, nor will I try to use anyone else's username and password
- I will report immediately any illegal, inappropriate or harmful material or incident I become aware of, to the Online Safety Manager or in their absence another DSL.

1.4 **I will be professional in my communications and actions when using the Meath School IT systems:**

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital images. I will not use my personal equipment to record these images unless I have permission

to do so. Where these images are published (e.g. on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.

- I will only use chat and social networking sites in school in accordance with the school's policies

- I will only communicate with pupils and parents / carers using official Meath School systems. Any such communication will be professional in tone and manner. I will not use social networking to make friends with pupils/parents/carers and will not share information relating to the children

- I will not engage in any on-line activity that may compromise my professional responsibilities

1.5 Meath School and I CAN have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- I will only use my personal mobile IT devices as agreed in the Meath School Online Safety policy and then in the same way as if I was using school equipment. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses.

- My personal mobile IT devices will be password protected

- I will not use personal email addresses when working with the children

- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes

- I will ensure that my data is regularly backed up in accordance with relevant Meath School policies

- I will not try to upload, download, or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work

- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies

- I will not disable or cause any damage to school equipment, or the equipment belonging to others

- I will only transport, hold, disclose, or share personal information about myself or others, as outlined in the School Personal Data Policy. Where personal data is transferred outside the secure school network, it must be encrypted

- I understand that Data Protection policy requires that any Staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority

- Images of pupils/Staff will only be stored/used in line with the Data Protection policy and with parent/carer/Staff consent

- I will immediately report any damage or faults involving equipment or software, however this may have happened

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

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

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

- I understand that this Acceptable Use Policy applies not only to my work and use of Meath School IT equipment in school, but also applies to my use of school IT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could involve a warning, a suspension, referral to HR and in the event of illegal activities. the involvement of the Police
- I understand that it is a criminal offence to use school IT systems for a purpose not permitted by its owner
- I understand that I must adhere to the requirements of the GDPR GDPR Regulations

I have read and understand the above and agree to use the school IT systems (both in and out of school) within these guidelines.

Staff / volunteer Name:	
Signed:	
Date:	

ANNEX D TO ONLINE SAFETY POLICY

MEATH SCHOOL

ACCEPTABLE USER POLICY AGREEMENT AND PERMISSION FORM – PARENT/CARER

1.1 Technology has transformed learning, entertainment and communication for individuals and for all organisations that work with young people. However, the use of technology can also bring risks. All users should have an entitlement to safe internet access at all times. This Meath School Acceptable Use Policy is intended to ensure:

- That young people will be responsible users and stay safe while using IT (especially the internet).
- That Meath School IT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- That parents/carers are aware of the importance of Online Safety and are involved in the education and guidance of young people with regard to their on-line behaviour

1.2 The school will try to ensure that pupils will have good access to ICT to enhance their learning and will, in return, expect them to agree to be responsible users.

1.3 Parents/carers are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Child's name	
Parent/Carer's name	
Parent/Carer's signature:	
Date:	

1.4 **Permission for my child to use the internet and electronic communication**

- As the parent / carer of the above pupil(s), I give permission for my son / daughter to have access to the internet and to ICT systems at school

- I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, Online Safety education to help them understand the importance of safe use of IT – both in and out of school

- I understand that Meath School will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and IT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies
- I understand that my son's / daughter's activity on the IT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy
- I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's Online Safety.

Parent/Carer's signature:	
Date:	

1.5 **Permission to publish my child's work (including on the internet)**

- It is Meath School's policy that, from time to time, it will publish the work of pupils by way of celebration. This includes on the internet, via the school website and in the school's virtual learning environment (VLE)

1.6 As the parent / carer of the above child I give my permission for this activity.

Parent/Carer's signature:	
Date:	

Your agreement of consent will carry through the school. If your circumstances change it is your responsibility to inform the school.

Meath School's Online Safety policy, which contains this Acceptable Use Policy Agreement, and the one signed by your child (to which this agreement refers), is available on the school website.

ANNEX E TO ONLINE SAFETY POLICY

MEATH SCHOOL
ACCEPTABLE USER POLICY AGREEMENT – COMMUNITY USER

1.1 You have asked to make use of our school's IT facilities. Before we can give you a log-in to our system we need you to agree to this acceptable use policy.

1.2 **For my professional and personal safety:**

- I understand that the school will monitor my use of the IT systems, email and other digital communications
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password
- I will report immediately any illegal, inappropriate, or harmful material or incident, of which I become aware, to a member of the Meath School Staff

1.3 **I will be professional in my communications and actions when using Meath School IT systems:**

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions

1.4 **Meath School and Surrey County Council have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:**

- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act (1959) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, except with the specific approval of the school
- I will not disable or cause any damage to school equipment, or the equipment belonging to others
- I will immediately report any damage or faults involving equipment or software, however this may have happened

I have read and understand the above and agree to use the school IT systems (both in and out of school) within these guidelines. I understand that failure to comply with this

agreement will result in my access to the school's IT system being withdrawn.

Community Username:	
Signed:	
Date:	

ANNEX F TO ONLINE SAFETY POLICY

GUIDANCE FOR REVIEWING WEBSITES

1.1 This guidance is intended for use when the school needs to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might typically include cyber-bullying, harassment, anti-social behaviour and deception. These may appear in emails, texts, social networking sites, messaging sites, gaming sites or blogs etc.

1.2 **Do not follow this procedure if you suspect that the web site(s) concerned may contain child abuse images. If this is the case, please refer to the Flowchart at Annex A for responding to online safety incidents and report immediately to the Police. Please follow all steps in this procedure:**

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

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

1.2 Ways of reporting potentially harmful websites for staff, parents and children, can be found through SWGfL on REPORT HARMFUL CONTENT

ANNEX F TO ONLINE SAFETY POLICY

CRITERIA FOR WEBSITE FILTERING

A. ORIGIN - What is the website's origin?

- The organisation providing the site is clearly indicated.
- There is information about the site's authors (about us, our objectives, etc.)
- There is a contact for further information and questions concerning the site's information and content.

B. DESIGN - Is the website well designed? Is it / does it:

- appealing to its intended audience (colours, graphics, layout)?
- easy to navigate through the site - links are clearly marked etc?
- have working links?
- Have inappropriate adverts?

C. CONTENT - Is the website's content meaningful in terms of its educational value?

- The site is free of spelling mistakes, grammatical errors, syntax errors, or typos.
- The site promotes equal and just representations of racial, gender, and religious issues.
- The site does not contain inappropriate content such as pornography, abuse, racial hatred and terrorism.
- The site does not link to other sites which may be harmful / unsuitable for the pupils
- Is the website current?

D. ACCESSIBILITY - Is the website accessible?

- Loads quickly?
- Does the site require registration or passwords to access it?
- The site does not require usage fees to be paid.