WESTBROOK OLD HALL PRIMARY SCHOOL

E-SAFETY/ONLINE POLICY

Our Best Preparation for Tomorrow
Is Doing Our Best Today

Westbrook Old Hall
PRIMARY SCHOOL

SCHOOL MISSION STATEMENT

We believe that the best preparation for tomorrow's future is striving to do our best today.

We believe that because our children matter, they have the right to be safe and healthy, happy and confident, recognised for the individuals they are and for those they might become.

We believe that because our children's achievement matters, they have the right to an excellent learning environment that promotes high expectations, ensures inclusion, recognises diversity and promotes progress and attainment.

We believe that because our children's future matters, they have the right to lead, the right to follow, the right to take best advantage of present and future technology and the right to a global life free from threat

Aims (Outcomes)

Our school aims that all children:

- Are tolerant and responsible
- Are happy and confident
- Are safe and healthy
- Are skilled and willing
- Are eco aware
- Are techno 'cute'
- Are leaders and partners
- Are flexible
- Are given every opportunity to attain and progress
- Are mindful of the joy of diversity
- Are focussed on being excellent in all they do
- Are expected always to do their best

SCHOOL AIMS

Our children matter, as does their achievement and so too does their future.

Because our children matter, we will work to:

- Ensure they are safe and ensure that they can keep themselves and others safe too
- Make sure that school life is happy, enjoyable and rewarding – taking each and every opportunity to build confident, positive citizens of the future
- Develop individuals with a sense of responsibility to themselves and to their community, able to respond positively to different views and beliefs

Because our children's achievement matters, we will work to:

- Release and develop the excellence latent in all our children
- Ensure high expectations in all we do, developing a culture that remains positive about the steps to success and able to celebrate success accordingly
- Provide an inclusive learning framework where individual needs are recognised and catered for, where diversity is celebrated for what it offers our school community
- Ensure that all children make good progress leading to attainment appropriate to potential
- Develop learners with a love of learning and a commitment to future learning in life

Because our children's futures matter, we will work to:

- Develop their ability to release the opportunities provided by technologies present and future
- Develop their awareness of their footprint upon this 'one' world and how they can contribute to its sustainability
- Develop a skills base and a solution-focussed attitude that can be applied to effect in a variety of circumstances now and in the future
- Develop an ability to lead others and to be led by others in productive working partnerships

EQUALITY STATEMENT

Equal Opportunities is the responsibility of the whole school community and must be reflected throughout the organisation of the school and be addressed in the taught and hidden curriculum.

All staff, governors, parents/guardians and pupils will be involved in developing, implementing and monitoring the equal opportunities policy and practice.

All staff, governors, parents/guardians and pupils regardless of race, religion, ethnicity, disability, age, gender, gender identity, sexual orientation, pregnancy or maternity and socio-economic background, are welcome and will be encouraged to participate in the life of the school.

The school recognises its responsibilities under the Equality Act 2010 to eliminate discrimination and to promote good race relations.

This policy has been equality impact assessed and we believe that it is in line with the Equality Act 2010 as it is fair, it does not prioritise or disadvantage any pupil and it helps to promote equality at this school.

BRITISH VALUES

The government set out its definition of British Values in the 2011 Prevent Strategy. At Westbrook Old Hall we reinforce regularly the following values through an agreed programme: Democracy, The Rule of Law, Individual Liberty, Mutual Respect and Tolerance of those of Different Faiths and Beliefs.

Background/Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school eSafety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the headteacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- 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 the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this eSafety policy is used in conjunction with other school policies (eg behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The eSafety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents/carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Development, Monitoring, Review of this Policy

This eSafety policy has been discussed and developed by a working group/committee made up of:

- DSL for Child Protection – Mr S Quinn/ Deputy DSL Mrs L Johnson
- Headteacher – Mr S Quinn
- eSafety Officer – Miss C Gavin
- ICT Leader – Miss C Gavin
- Teachers
- Support Staff
- ICT Technical staff – EDAC
- Governors

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

- Staff meetings
- INSET Day
- Governors meeting/committee meeting

Schedule for Development, Monitoring, Review

This eSafety policy was approved by the Governing Body/Governors Sub Committee on:	21/06/12 Reviewed September 2020
The implementation of this eSafety policy will be monitored by the:	Carla Gavin (ICT Leader) Stewart Quinn (Headteacher) DSL, Louise Johnson Deputy DSL, Gavin Brown (Chair of Governors) Carla Gavin E-Safety Officer, Kerrie Murray E-Safety Governor
Monitoring will take place at regular intervals:	Termly
The Governing Body/Governors Sub Committee will receive a report on the implementation of the eSafety policy generated by the monitoring group (which will include anonymous details of eSafety incidents) at regular intervals:	Termly in head's report and in Full Governor Meetings
The eSafety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to eSafety or incidents that have taken place. The next anticipated review date will be:	Annually
Should serious eSafety incidents take place, the following external persons/ agencies should be informed:	MAT CEO, MAT ICT Manager, LA Safeguarding Team, Police Commissioner's Office

The school will monitor the impact of the policy using:

- Logs of reported incidents

- eSafety meeting with headteacher, eSafety leader, eSafety governor

- Surveys/questionnaires of
  - pupils
  - parents/carers
  - staff

Scope of the Policy

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

The Education and Inspections Act 2006 empowers headteachers, 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 eSafety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

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

Roles and Responsibilities

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

Governors:

Governors are responsible for the approval of the eSafety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors/ Governors Sub Committee receiving regular information about eSafety incidents and monitoring reports. A member of the Governing Body has taken on the role of eSafety Governor. The eSafety Governor will have a separate role to the ICT Link Governor. The role of the eSafety Governor will include:

- regular meetings with the designated eSafety Officer and Designated Safeguarding Lead
- regular monitoring of eSafety incident logs
- reporting to relevant Governors committee/meeting

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including eSafety) of members of the school community, though the day to day responsibility for eSafety will be delegated to the eSafety Officer.
- The Headteacher/Senior Leaders are responsible for ensuring that the eSafety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their eSafety roles and to train other colleagues, as relevant
- The Headteacher/Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal eSafety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the eSafety Officer.
- The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious eSafety allegation being made against a member of staff. (see WBC flow chart on dealing with eSafety incidents)

Designated eSafety Officer:

- leads the eSafety committee
- takes day to day responsibility for eSafety issues and has a leading role in establishing and reviewing the school eSafety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an eSafety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority/MAT
- liaises with school ICT technical staff
- receives reports of eSafety incidents and creates a log of incidents to inform future eSafety developments,
- meets regularly with eSafety Governor to discuss current issues, review incident logs and filtering/change control logs
- attends relevant meeting/committee of Governors
- reports regularly to Senior Leadership Team

Network Manager/Technical staff:

The Network Manager/Systems Manager/ICT Technician/ICT Co-ordinator is responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the eSafety technical requirements as advised by Becta and the Acceptable Use Policy.
- the school's filtering policy (if it requires one), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that he/she keeps up to date with eSafety technical information in order to effectively carry out their eSafety role and to inform and update others as relevant
- that the use of the network/Learning Platform/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the eSafety Co-ordinator/Headteacher/Senior Leader/Head of ICT/ ICT Co-ordinator/Class teacher/Head of Year (as in the section above) for investigation/action/sanction
- that monitoring software/systems are implemented and updated as agreed in school policies

Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of eSafety matters and of the current school eSafety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy/Agreement (AUP)
- they report any suspected misuse or problem to the eSafety Officer/Headteacher/ (as in the section above) for investigation/action/sanction
- digital communications with pupils and parents (email/Learning Platform) should be on a professional level and only carried out using official school systems
- eSafety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the school eSafety and acceptable use policy
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra-curricular and extended school activities
- they are aware of eSafety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices

- in lessons where internet use is pre-planned 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

Designated Safeguarding Leads

should be trained in eSafety issues and be aware of the potential for serious child protection issues to arise from:

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

eSafety Committee

Members of the eSafety committee (or other relevant group) will assist the eSafety Coordinator with:

- the production/review/monitoring of the school eSafety policy/documents.
- the production/review/monitoring of the school filtering policy (if the school chooses to have one)

Pupils:

- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems. At KS1 it would be expected that parents/carers would sign on behalf of the pupils.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking/use of images and on cyber-bullying.
- should understand the importance of adopting good eSafety practice when using digital technologies out of school and realise that the school's eSafety Policy covers their actions out of school, if related to their membership of the school

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website/Learning Platform and information about national/local eSafety campaigns/literature. Parents and carers will be responsible for:

- endorsing (by signature) the Pupil Acceptable Use Policy
- accessing the school website/Learning Platform/online pupil records in accordance with the relevant school Acceptable Use Policy.

Policy Statements

Education – Pupils

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 eSafety is therefore an essential part of the school's eSafety provision. Children and young people need the help and support of the school to recognise and avoid eSafety risks and build their resilience. eSafety education will be provided in the following ways:

- A planned eSafety programme should be provided as part of ICT/PSHE/other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Key eSafety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities/e-safety week
- Pupils should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information
- Pupils should be helped to understand and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems/internet will be posted in all rooms
- Staff should act as good role models in their use of ICT, the internet and mobile devices

Education – parents/carers

Many parents and carers have only a limited understanding of eSafety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online experiences. 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. "There is a generational digital divide". (Byron Report).

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

- Letters, newsletters, web site, learning platform
- Parents' evenings
- E-Safety Workshops

Education - Extended Schools

Messages to the public around e safety should also be targeted towards grandparents and other relatives as well as parents. 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.

Education & Training – Staff

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

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

- All new staff should receive eSafety training as part of their induction programme, ensuring that they fully understand the school eSafety policy and Acceptable Use Policies
- The eSafety Officer will receive regular updates through attendance at LA/other information/training sessions and by reviewing guidance documents released by BECTA/WBC and others.
- This eSafety policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days.
- The eSafety Leader will provide advice/guidance/training as required to individuals as required

Training – Governors

Governors should take part in eSafety training/awareness sessions, with particular importance for those who are members of any committee/group involved in ICT/eSafety/health and safety/child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/National Governors Association or other relevant organisation.
- Participation in school training/information sessions for staff or parents

Technical – infrastructure/equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their eSafety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the eSafety technical requirements outlined by Becta and the Acceptable Usage Policy
- School ICT systems must be regularly updated to ensure up-to-date anti-virus definitions and Microsoft Windows Security Updates are installed. Essential software i.e. Acrobat Reader, Flash Player, Java, Internet Explorer, Smartboard etc. must be kept current.
- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually, by the eSafety Committee
- All users will be provided with a username and password to access the school network who will keep an up to date record of users and their usernames.
- All users of the school learning platform will be provided with a username and password for secure access in school and beyond.
- The "master/administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader.
- School Data should be securely managed when taken off the school site using encrypted memory devices or password protected files.
- Users will be made responsible for the security of their username and password; they must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by Omega MAT
- The school has provided enhanced user-level filtering through the use of the filtering programme provided by Omega MAT.

- In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher (or other nominated senior leader).
- Any filtering issues should be reported immediately to the IT team at Omega MAT.
- Requests from staff for sites to be added or removed from the filtered list will be considered at the appropriate senior level If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the eSafety Committee
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- An appropriate system is in place for users to report any actual/potential eSafety incident to the designated eSafety Officer.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed system is in place (e-safety officer to provide access) for the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the school system.
- An agreement is in place (see Staff AUP)) that allows/forbids staff from installing programmes on school workstations/portable devices.
- An agreement is in place (see Staff AUP) regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school workstations/portable devices.

Curriculum

eSafety should be a focus in all areas of the curriculum and staff should reinforce eSafety messages in the use of ICT across the curriculum:

- eSafety should be taught regularly through a scheme of work with identified progression of knowledge, skills and understanding.
- eSafety skills should be embedded through both discrete ICT and cross-curricular application.
- 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.
- Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites visited and encourage children to use child friendly search engines.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that they can temporarily be removed from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- Pupils should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Use of digital and video images – Photographic/ Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on 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.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website *(see Parent Photograph consent form)*

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system (personal laptops must not be used) or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected (many memory sticks/cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device once it has been transferred or its use is complete.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

	Staff / Other Adults				Pupils			
Communication Technologies (outside of those available on the learning platform)	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	✓						✓ (Year 6)	✓
Use of personal mobile phones in lessons				✓				✓
Use of personal mobile phones in social time	✓							✓
Taking photos on personal mobile phones or other camera devices				✓				✓
Use of personal devices e.g. laptops, netbooks, PDAs, PSPs, iPad, iPod		✓		✓				✓
Use of personal email addresses in school, or on school network		✓						✓
Use of removable data pens e.g. USB sticks	✓							✓
Use of school email for personal emails				✓				✓

Use of chat rooms/facilities				✓				✓
Use of instant messaging				✓				✓
Use of social networking sites				✓				✓
Use of blogs	✓						✓	

When using communication technologies, the school considers the following as good practice:

- Where available the official school email service may be regarded as safe and secure and is monitored. Staff should therefore use only the school email service to communicate with other professionals and parents.
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person – 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.
- 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 email systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Unsuitable/inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts certain internet usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
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**				✓	✓
	promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation				✓	✓
	adult material that potentially breaches the Obscene Publications Act in the UK				✓	✓
	criminally racist material in UK				✓	✓
	pornography				✓	

	promotion of any kind of discrimination				✓	
	promotion of racial or religious hatred				✓	
	threatening behaviour, including promotion of physical violence or mental harm				✓	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				✓	
Using school systems to run a private business					✓	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Omega MAT and/or the school					✓	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					✓	
Revealing or publicising confidential or proprietary information (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					✓	
Online gaming (educational)					✓	
Online gaming (non-educational)					✓	
Online gambling					✓	
Online shopping/commerce					✓	
File sharing					✓	
Use of social networking sites					✓	
Use of video broadcasting e.g. YouTube					✓	

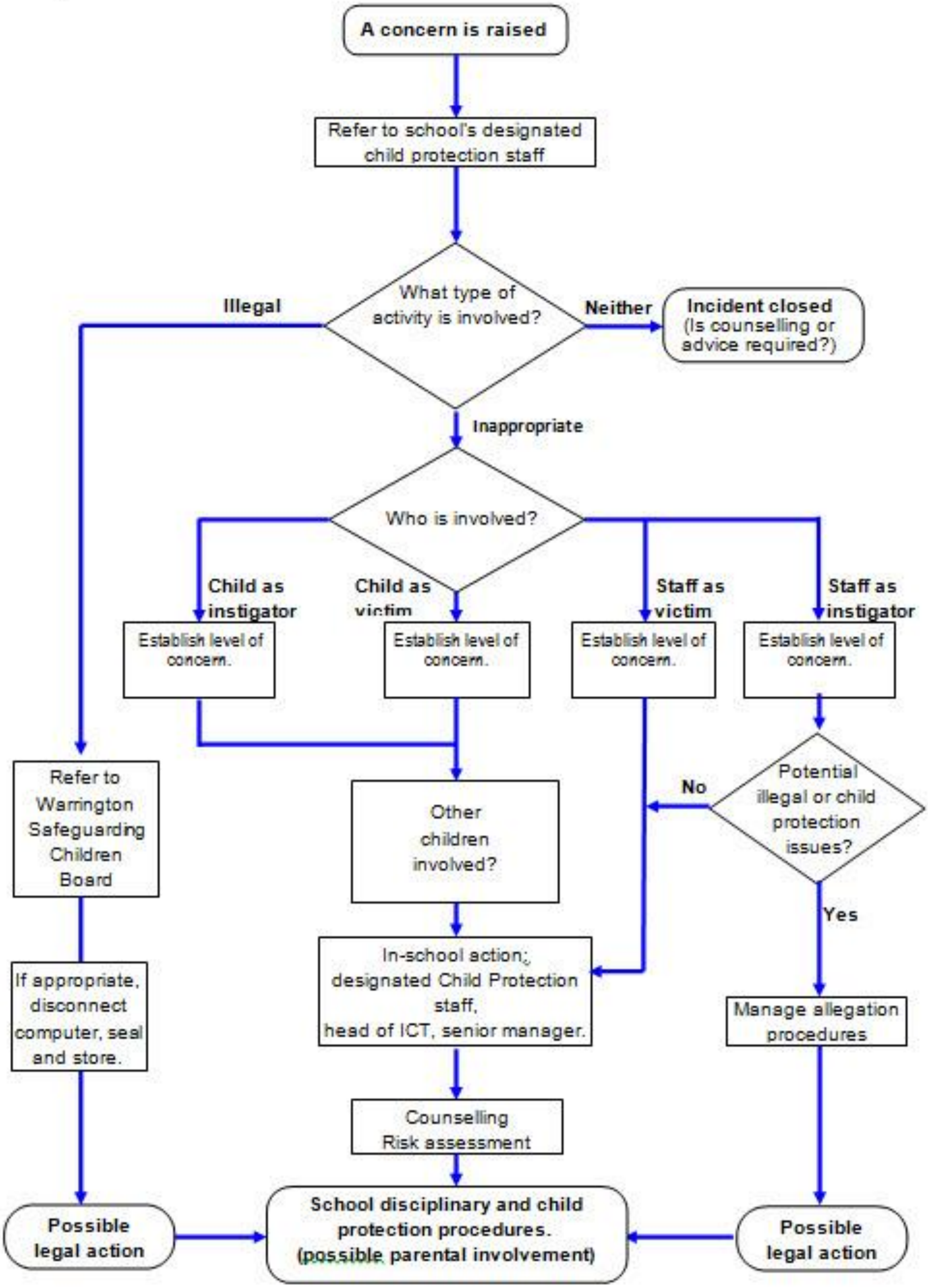
Responding to incidents of misuse

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 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:

- If any apparent or actual misuse appears to involve illegal activity i.e.
- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

The following flow chart below should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.

Response to an incident of concern


A concern is raised
Refer to school's designated child protection staff
What type of activity is involved?
Illegal
Neither
Incident closed (Is counselling or advice required?)
Inappropriate
Who is involved?
Child as instigator
Child as victim
Staff as victim
Staff as instigator
Establish level of concern.
Establish level of concern.
Establish level of concern.
Establish level of concern.
Refer to Warrington Safeguarding Children Board
Other children involved?
No
Potential illegal or child protection issues?
Yes
If appropriate, disconnect computer, seal and store.
In-school action; designated Child Protection staff, head of ICT, senior manager.
Manage allegation procedures
Counselling Risk assessment
Possible legal action
School disciplinary and child protection procedures. (possible parental involvement)
Possible legal action

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. It is recommended that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer.

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

Pupils **Actions/Sanctions**

Incidents:	Refer to class teacher/ tutor	Refer to ICT Leader	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re. filtering/security etc.	Inform parents /carers	Removal of network/ internet access rights	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 or accessing the school network, using another student's/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	✓	✓	✓					✓	✓

Staff **Actions / Sanctions**

Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority/ HR	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 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	✓	✓	✓	✓	✓	✓	✓	✓