On-line Safety Policy

Tenbury Primary Academy

‘Therefore encourage one another and build each other up.

1 Thessalonians 5:11

Last updated: March 2025

Date for review: March 2026

Introduction

National guidance suggests that it is essential for schools to take a leading role in online safety. Becta in its "Safeguarding Children in a Digital World" suggested:

> *"That schools support parents in understanding the issues and risks associated with children's use of digital technologies. Furthermore, Becta recommends that all schools have acceptable use policies, and ensure that parents are aware of the procedures for online safety within the school. Recognising the growing trend for home-school/academy links and extended school activities, Becta recommends that schools take an active role in providing information and guidance for parents on promoting online safety messages in home use of ICT, too."*

The Byron Review "Safer Children in a Digital World" stressed the role of schools:

> *"One of the strongest messages I have received during my Review was about the role that schools and other services for children and families have to play in equipping children and their parents to stay safe online. To empower children and raise the skills of parents, I make recommendations to Government in the following areas: delivering online safety through the curriculum, providing teachers and the wider children's workforce with the skills and knowledge they need, reaching children and families through Extended School and taking steps to ensure that Ofsted holds the system to account on the quality of delivery in this area."*

DfE guidance, 'Teaching Online Safety in School', published June 2019, states:

> ***"It is important to teach pupils about the underpinning knowledge and behaviours that can help pupils navigate the online world safely and confidently, regardless of the device, platform or app."***

Academies are expected, by Ofsted, to evaluate their level of online safety (for example using the 360°Safe self-review framework or similar tool) and online safety is now subject to an increased level of scrutiny during inspections.

Several of the statements below can be directly related to aspects of online safety:

Behaviour and safety of pupils at the school

When evaluating the behaviour and safety of pupils, inspectors consider:

- pupils' attitudes to learning and conduct in lessons and around the establishment
- pupils' behaviour towards, and respect for, other young people and adults, including freedom from bullying and harassment that may include cyber-bullying and prejudice-based bullying related to special educational need, sexual orientation, sex, race, religion and belief, gender reassignment or disability
- how well teachers manage the behaviour and expectations of pupils to ensure that all pupils have an equal and fair chance to thrive and learn in an atmosphere of respect and dignity
- pupils' ability to assess and manage risk appropriately and to keep themselves safe
- pupils' attendance and punctuality at school/academy and in lessons
- how well the school/academy ensures the systematic and consistent management of behaviour.

The Computing curriculum contains specific references to online safety:

- **KS1**: use technology safely and respectfully, keeping personal information private; know where to go for help and support when they have concerns about material on the internet
- **KS2**: use technology safely, respectfully and responsibly; know a range of ways to report concerns and inappropriate behaviour.

Background and rationale

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

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

- Access to illegal, harmful or inappropriate images or other content
- Allowing or seeking unauthorised access to personal information
- Allowing or seeking unauthorised access to private data, including financial data
- The risk of being subject to grooming 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 or addictive use which may impact on social and emotional development and learning.
- The potential to be drawn into terrorism through radicalisation via social media

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

Our On-line Safety Policy has been written from a template provided by Worcestershire County Council which has itself been derived from that provided by the South West Grid for Learning.

Policy and leadership

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

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

Responsibilities: Online Safety Coordinator

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

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school/academy online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident
- provides training and advice for staff
- liaises with the Local Authority and DHMAT
- liaises with academy ICT technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- reviews weekly the output from monitoring software and initiates action where necessary
- meets regularly *termly* with online safety governor to discuss current issues and review incident logs
- attends relevant meetings and committees of Governing Body
- reports regularly to Senior Leadership Team
- receives appropriate training and support to fulfil their role effectively

The online safety co-ordinator at Tenbury Primary Academy is Mrs Kerri Phelps.

Responsibilities: governors

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

- *termly meetings with the Online safety Co-ordinator with an agenda based on:*
    - *monitoring of online safety incident logs*
    - *reporting to relevant Governors committee / meetings*

The online safety governor at Tenbury Primary Academy is Mr Mark Yarnold

Responsibilities: Head teacher

- The Head teacher, as the Online Safety Co-ordinator, is responsible for ensuring the safety (including online safety) of all members of the academy community.
- The Head teacher and another member of the senior management team are familiar with the procedures to be followed in the event of a serious online safety allegation being made against a member of staff, including non-teaching staff. (see flow chart on

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

Responsibilities: classroom based staff

Teaching and Support Staff are responsible for ensuring that:

- they safeguard the welfare of pupils and refer child protection concerns using the proper channels: **this duty is on the individual, not the organisation or the academy**.
- they follow all relevant guidance and legislation including, for example, Keeping Children Safe in Education and UK GDPR regulations
- all digital communications with learners, parents and carers and others are on a professional level and only carried out using official school systems and devices (where staff use AI, they should only use school-approved AI services for work purposes which have been evaluated to comply with organisational security and oversight requirements
- they have an up to date awareness of online safety matters and of the current academy online safety policy and practices, including the academy's approach to the Prevent Agenda.
- they are able to identify children who may be vulnerable to radicalisation, and know what to do when they are identified
- they have read, understood and signed the academy's Acceptable Use Agreement for staff.
- they report any suspected misuse or problem to the Online safety Co-ordinator/Headteacher
- they embed online safety issues in the curriculum and other activities, also acknowledging the planned online safety programme (see section C)
- they adhere to the school's technical security policy, with regard to the use of devices, systems and passwords and have an understanding of basic cybersecurity
- they have a general understanding of how the learners in their care use digital technologies out of school, in order to be aware of online safety issues that may develop from the use of those technologies, including 'sexting', the use of Virtual Reality and use of self-generated images.
- they are aware of the benefits and risks of the use of Artificial Intelligence (AI) services in school, being transparent in how they use these services, prioritising human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans, fact-checked and critically evaluated.

Responsibilities: ICT technician

The ICT Technician is responsible for ensuring that:

- the academy's ICT infrastructure and data are secure and not open to misuse or malicious attack
- the academy meets the online safety technical requirements outlined in section B.2.2 of this policy (and any relevant Local Authority Online safety Policy and guidance)

- users may only access the academy's networks through a properly enforced password protection policy as outlined in the school/academy's e-security policy
- shortcomings in the infrastructure are reported to the ICT coordinator or head teacher so that appropriate action may be taken.

Policy development, monitoring and review

This online safety policy has been developed (from a template provided by Worcestershire County Council) in consultation with:

- *Online safety Coordinator*
- *Designated Safeguarding Leads*
- *Head teacher / Senior Leaders*
- *Teachers*
- *Support Staff*
- *ICT Technical staff*
- *Governors (especially the online safety governor)*
- *Parents and Carers*
- *Pupils*

  Our whole school policy is communicated with all stakeholders in the following ways
- *Staff meetings*
- *School Council*
- *INSET Days*
- *Governor's meetings*
- *Parents' evening*
- *Academy website / newsletters*

Acceptable Use Agreements

All members of the academy community including technicians, whether directly employed or from external technical support teams, are responsible for using the academy ICT systems in accordance with the appropriate Acceptable Use Agreement (AUA), which they ARE expected to sign before being given access to academy systems.

Acceptable Use Agreements are provided for:

- Pupils
- Staff (and volunteers)
- Parents / carers

Acceptable Use Agreements are introduced at parents' induction meetings and signed by all pupils as they enter school/academy (with parents possibly signing on behalf of children below Year 2).

Pupils re-sign on entering a new Key Stage.

All employees of the academy and volunteers sign when they take up their role and in the future if significant changes are made to the policy.

Parents sign once when their child enters the academy. The parents' policy also includes permission for use of their child's image (still or moving) by the academy, permission for their child to use the academy's ICT resources (including the internet) and permission to publish their work.

Self Evaluation

Evaluation of online safety is an ongoing process and links to other self-evaluation tools used in our academy, in particular pre Ofsted evaluations along the lines of the Self Evaluation Form (SEF). The views and opinions of all stakeholders (pupils, parent, teachers …) are taken into account as part of regular questionnaires.

Tenbury CE Primary Academy also uses the 360 degree safe Self-review Tool from the UK Safer Internet Centre which, in turn, informs any online safety actions on our annual Safeguarding Action Plan. Our last self-review was in December 2023, where we have reached a high enough level in all areas to apply for the Online Safety Mark.

Whole School approach and links to other policies

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

Core ICT policies

Computing Policy	How ICT is used, managed, resourced and supported in our academy.
Online Safety Policy	How we strive to ensure that all individuals in academy stay safe while using Learning Technologies. The online safety policy constitutes a part of the ICT policy.
Data Protection Policy	How we categorise, store and transfer sensitive and personal data and protect systems. This links strongly and overlaps with the online safety policy.

Other policies relating to online safety

Anti-bullying	How your academy strives to eliminate bullying – link to cyber bullying
PSHE	Online safety has links to staying safe
Safeguarding	Safeguarding pupils electronically is an important aspect of Online safety. ***The online safety policy forms a part of the academy's safeguarding policy***
Behaviour	Positive strategies for encouraging online safety and sanctions for disregarding it.
Use of images	**WCC guidance to support the safe and appropriate use of images in schools, academies and settings**
Remote Learning Policy	**Following Covid 19 lockdowns, this policy provides information on how remote learning will be successfully and safely delivered.**

Illegal or inappropriate activities and related sanctions

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

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

- **child sexual abuse images (illegal - The Protection of Children Act 1978)**
- **grooming, incitement, arrangement or facilitation of sexual acts against children (illegal – Sexual Offences Act 2003)**
- **possession of extreme pornographic images (illegal – Criminal Justice and Immigration Act 2008)**
- **criminally racist material in UK – to stir up religious hatred including radicalisation as per the Prevent Agenda (or hatred on the grounds of sexual orientation) (illegal – Public Order Act 1986)**
- pornography
- promotion of any kind of discrimination
- promotion of racial or religious hatred
- threatening behaviour, including promotion of physical violence or mental harm
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school/academy or brings the school/academy into disrepute

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

- *Using academy systems to undertake transactions pertaining to a private business*
- *Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Worcestershire County Council Broadband and the academy.*
- *Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions*
- *Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)*
- *Creating or propagating computer viruses or other harmful files*
- *Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files that causes network congestion and hinders others in their use of the internet)*
- *On-line gambling and non-educational gaming*
- *On-line shopping / commerce unless directly related to school/academy business*
- *Use of social networking sites*

If members of staff suspect that misuse might have taken place – whether or not it is evidently illegal (see above) - it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. Please see Appendix 2.

It is more likely that the academy 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 academy 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 indicated on the following pages:

Pupil sanctions

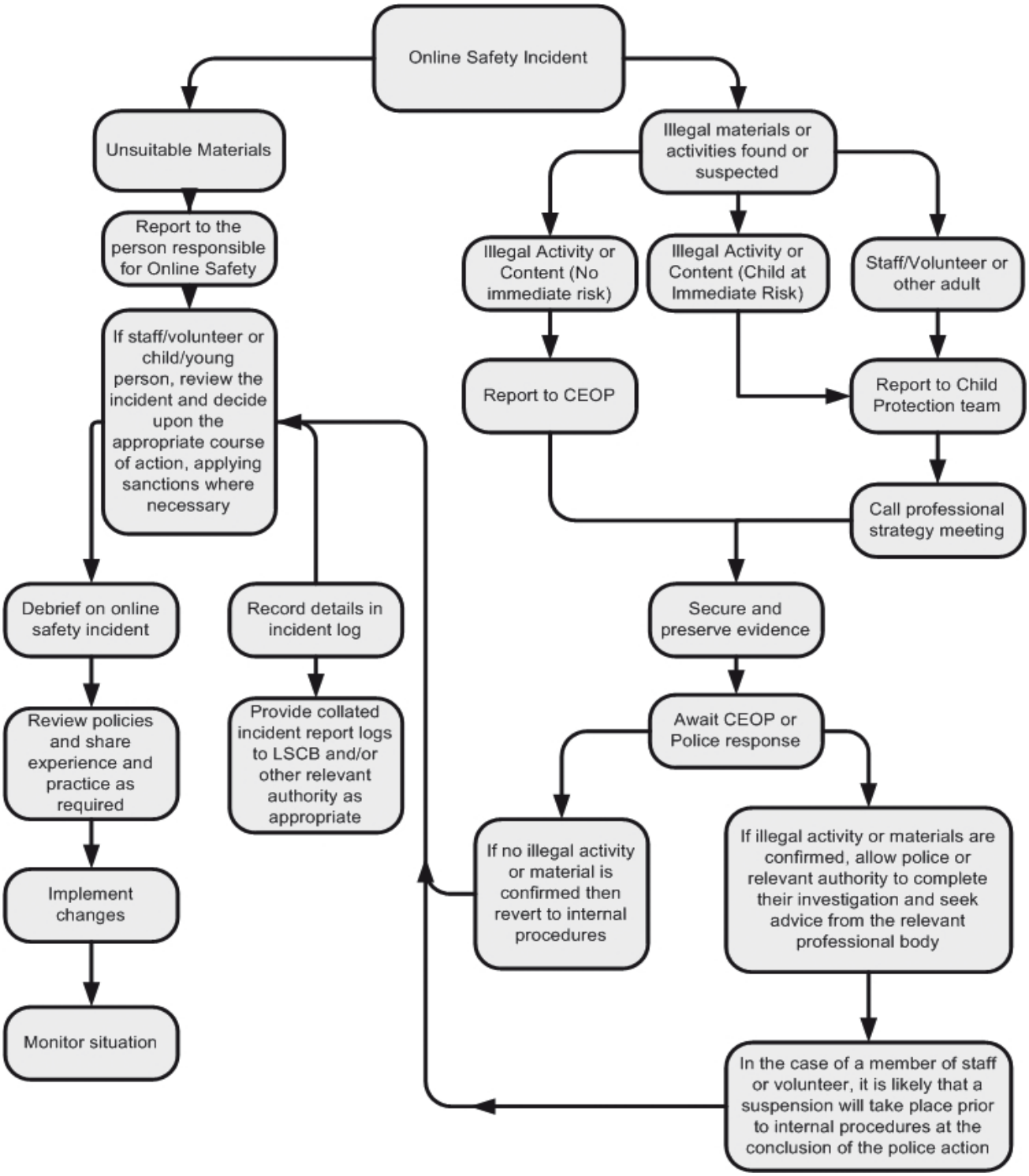
	Refer to:					Inform:	Action:		
	Class teacher	Online safety coordinator	Refer to head teacher	Refer to Police	Refer to online safety coordinator for action re filtering / security etc	Parents / carers	Remove of network / internet access rights	Warning	Further sanction e.g. detention / exclusion
Deliberately 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/academy network by sharing username and passwords	✔	✔	✔		✔		✔	✔	
Attempting to access the school/academy network, using another pupil's account	✔				✔		✔		
Attempting to access or accessing the school/academy 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/academy into disrepute or breach the integrity of the ethos of the school/academy	✔		✔					✔	
Using proxy sites or other means to subvert the school/academy'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 sanctions

	Refer to:					Action:		
	E safety	Head teacher	Local Authority / HR/ DHMAT	Police	Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	✔	✔	✔	✔	✔		✔	✔
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	✔	✔				✔		
Unauthorised downloading or uploading of files	✔				✔	✔		
Allowing others to access school/academy network by sharing username and passwords or attempting to access or accessing the school/academy 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/academy into disrepute or breach the integrity of the ethos of the school/academy	✔		✔			✔		
Using proxy sites or other means to subvert the school/academy'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	✔	✔	✔		✔			✔

Reporting of online safety breaches

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



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

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

- *Members of staff are permitted to bring their personal mobile devices into school provided they are kept out of sight. They are required to use their own professional judgement as to when it is appropriate to use them. Broadly speaking this is:*
  - ✓ *Personal hand held devices will be used in lesson time only in an emergency or extreme circumstances*
  - ✓ *Members of staff are free to use these devices outside teaching time in areas such as the Staffroom, however must take care not to use them when in areas where there may be children present e.g. school corridors..*
- *Pupils are not currently permitted to bring their personal hand held devices into school, unless expressly requested by a parent if the child is walking home alone at the end of the day and they feel they need to have access to their mobile phone. If anybody does, they are removed and kept in the School office until the end of the day.*
- *Pupils are not currently permitted to have other electronic devices, such as smart watches, with imaging and sharing capabilities, in our school or Nursery either.*
- *A number of such devices are available in school (e.g. I Pads) and are used by pupils as considered appropriate by members of staff.*

	Staff / adults				Pupils			
Personal hand held technology	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff	Not allowed
Mobile phones may be brought into the academy	✔					✔		
Use of mobile phones in lessons				✔				✔
Use of mobile phones in social time		✔						✔
Taking photos on personal phones or other camera devices				✔				✔
Use of hand held devices e.g. PDAs, gaming consoles	✔						✔	

Use of communication technologies

Email

Access to email is provided for all academies using Worcestershire schools' broadband via their Global IDs.

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

- Staff and pupils should use only the academy email services to communicate with others regarding academy business when in academy, or on academy systems (e.g. by remote access)
- Users need to be aware that email communications may be monitored
- *Pupils normally use only a class email account to communicate with people outside academy and with the permission / guidance of their teacher*
- A structured education program is delivered to pupils which helps them to be aware of the dangers of and good practices associated with the use of email
- *Staff may only access personal email accounts on academy systems for emergency or extraordinary purposes (if they are not blocked by filtering)*
- Users must immediately report to their teacher / online safety coordinator – in accordance with this policy (see sections A.2.6 and A.2.7) - the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature. They must not respond to any such email.

	Staff / adults				Pupils			
Use of Email	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff	Not allowed
Use of personal email accounts in school/academy / on school/academy network		✔						✔
Use of school/academy email for personal emails		✔						✔

Social networking (including chat, instant messaging, blogging etc)

Use of social networking tools	Staff / adults				Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff	Not allowed
Use of non-educational chat rooms etc				✔				✔
Use of non-educational instant messaging				✔				✔
Use of non-educational social networking sites				✔				✔
Use of non-educational blogs				✔				✔

Videoconferencing

Videoconferencing equipment in classrooms must be switched off when not in use and not set to auto answer.

External IP addresses should not be made available to other sites.

Only web based conferencing products that are authorised by the academy (and are not blocked by internet filtering) are permitted for classroom use.

Videoconferencing must be supervised directly by a teacher.

Permission for pupils to take part in video conferences is sought from parents / carers at the beginning of the pupil's time in the academy. Only where permission is granted may pupils participate.

Only key administrators have access to videoconferencing administration areas.

Use of digital and video images

- 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.
- Members of staff are allowed to take digital still and video images to support educational aims, but must follow policies concerning the sharing, distribution and publication of those images. Those images should only be captured using academy equipment whenever possible.
- 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 academy into disrepute.
- Staff should be aware of pupils for whom it has been deemed inappropriate to take and share/publish their photograph (e.g. some looked after children) or where

parents/carers have not given consent. A class list is given to each teacher by the school office.

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

Use of web-based publication tools

Website

Our academy uses the public facing website www.tenburyceprimary.co.uk only for sharing information with the community beyond our academy. This includes, from time-to-time, celebrating work and achievements of pupils. All users are required to consider good practice when publishing content.

- Personal information will not be posted on the academy website
- *Only pupil's first names will be used on the website, and only then when necessary.*
- Photographs published on the website, or elsewhere, that include pupils will be selected carefully and will comply with the following good practice guidance on the use of such images:
    - ✓ pupils' full names will not be used anywhere on a website or blog, and never in association with photographs
    - ✓ *where possible, photographs will not allow individuals to be recognised*
- written permission from parents or carers will be obtained before photographs of pupils are published on the academy website
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Professional standards for staff communication

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

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

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

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

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

Infrastructure

Password security

All staff and pupils have their own global ID logon and own passwords for the various APPs we use such as Google Classroom, 'Timestables Rockstars' etc. Teaching in online safety lessons includes:

- understanding why passwords are important, how to keep them safe and to be aware that others may try to trick you into revealing them ie 'phishing' scams.
- the importance of online security to protect against viruses
- knowing what to do when a password is compromised or thought to be compromised

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

Filtering

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. No filtering system can, however, provide a 100% guarantee that it will do so. It is therefore important that the academy has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this academy.

Responsibilities

The day-to-day responsibility for the management of the academy's filtering policy is held by the **online safety coordinator** (with ultimate responsibility resting with the **Head teacher and governors**). They manage filtering in line with this policy and keep logs of changes to and breaches of the filtering system.

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

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

Education / training / awareness

Pupils are made aware of the importance of filtering systems through the academy's online safety education programme

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

- signing the Acceptable Use Agreement (as part of their induction process)
- briefing in staff meetings, training days, memos etc.
- **Parents** will be informed of the academy's filtering policy through the Acceptable Use Agreement and through *online safety awareness sessions / newsletter etc.*

Changes to the filtering system

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

- The teacher makes the request to the academy online safety coordinator.
- The online safety coordinator checks the website content to ensure that it is appropriate for use in academy.

THEN

- *If agreement is reached, the online safety coordinator makes a request to John Finch Computers and 'Securly', our filtering provider*
- *The team will endeavour to unblock the site within a reasonable time. This process can take a number of hours so teaching staff are required to check websites well in advance of teaching sessions. *This is also true for virtual meetings/CPD such as Teams or Zoom. Staff will need to inform John Finch Computers if they need a specific link made available or, after discussion with Mrs Phelps, use either the office or Headteacher's computer. Any online staff meetings are held via Google-Meet, which does not require JFC to unblock as the Google Classroom system has been set-up specifically for the Tenbury Primary Academy Network.*

The online safety coordinator will need to apply a rigorous policy for approving / rejecting filtering requests and this should be based on the site's content:

- 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 pupils.

Monitoring

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

Monitoring is carried out using the 'Securly' system and takes place as follows:

- The Headteacher is immediately sent an email by the system, if any serious breach of internet safety occurs
- At least 2 identified members of staff (deputy head and headteacher) review the monitoring captures weekly
- Potential issues are referred to an appropriate person depending on the nature of the capture.
- Teachers are encouraged to identify in advance any word or phrase likely to be picked up regularly through innocent use (e.g. 'goddess' is captured frequently when a class is researching or creating presentations on the Egyptians) so that the word can be allowed for the period of the topic being taught.

Audit / reporting

Filter control logs and incident logs are made available to:

- the online safety governor at termly Safeguarding Committee meetings
- the Worcestershire Safeguarding Children Board on request

This filtering policy will be reviewed, with respect to the suitability of the current provision, in response to evidence provided by the audit logs.

Technical security

See separate Security Policy

Personal data security (and transfer)

See separate Security Policy

Teachers frequently discuss issues relating to data security and how it relates to staying safe in and out of the academy. **The academy's Data Protection Officer is Mrs Lesley Newall.**

Education

Online safety education

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the academy's online safety provision. Children and young people need constant help and support to recognise and avoid online safety risks and build their resilience. This is particularly important for helping them to learn how to stay safe out of school where technical support and filtering may not be available to them.

Online safety education will be provided in the following ways:

- A planned online safety programme is provided as part of Computing, PHSE, **Relationships Education** and other lessons. This is regularly revisited, covering the use of ICT and new technologies both in academy and beyond academy. It is re-visited at least once a term:
    - **During National Anti-Bullying Week in November**
    - **During the week of National Internet Safety Day in February**
    - **During July, towards the end of term, in order to remind the children of online safety before the summer holiday.**
- Key online safety messages are reinforced through further input via assemblies and pastoral activities, as well as informal conversations when the opportunity arises.
- Pupils are helped to understand the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use of ICT both within and outside the academy.
- *In lessons where internet use is pre-planned, it is best practice that younger pupils should be guided to sites checked as suitable for their use.* Processes should be in place, and known to pupils, for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit, encouraging pupils to discuss anything of which they are unsure and implementing the expected sanctions and/or support as necessary.
- Pupils are made aware of what to do should they experience anything, while on the Internet, which makes them feel uncomfortable.
- A range of resources are used to support staff in online safety education including **CEOP resources, 'Be Internet Legends' by Google and 'Education for a Connected World'** which is a framework to equip children and young people for digital life, published by the UK Council for Child Internet safety (UKCCIS).

- All teaching staff have individual logins to Project EVOLVE to further enhance e-safety lessons in the curriculum.

The contribution of the pupils to the e-learning strategy

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

We have a Pupil Safety Committee who produce online safety posters and survey our pupils about their internet use annually

Staff training

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

- A planned programme of formal online safety training is made available to staff, which is repeated annually. The next training is planned for October 2025.
- *It is expected that some staff will identify online safety as a training need within the performance management process.*
- All new staff receive online safety training as part of their induction programme, ensuring that they fully understand the academy online safety policy and Acceptable Use Agreements, which are signed as part of their induction
- The Online safety Co-ordinator (or another member of staff such as the Safeguarding Officer) has completed basic CEOP training.
- *The Online safety Coordinator receives regular updates through attendance at local authority or other training sessions and by reviewing guidance documents released by the DfE, the local authority, OFSTED, the WSCB and others.*
- *All teaching staff have been involved in the creation of this online safety policy and are therefore aware of its content*
- *The Online safety Coordinator provides advice, guidance and training as required to individuals as required on an ongoing basis.*
- *External support for training, including input to parents, is sought from appropriately qualified persons when required.*

Governor training

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

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

The online safety governor works closely with the online safety coordinator/headteacher and reports back to the full governing body.

Parent and 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 their on-line 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 academy therefore seeks to provide information and awareness to parents and carers through:

- *Letters, newsletters, web site, Google Classroom*
- *Parents evenings*
- *Workshops*

Wider community understanding

The academy signposts members of the community to further information and resources on online safety on our website, so that parents and pupils can together gain a better understanding of these issues. **Safety information for parents/carers on our website includes sites/APPs such as TikTok, Fortnite, MOMO, Youtube, FIFA, Snapchat, WhatsApp, Roblox and Minecraft. In addition, Tenbury Primary Academy subscribes to a monthly online safety newsletter, which is published on our website each month for parents/carers. This covers a range of websites/APPS/issues, with helpful and practical advice. Tenbury Primary Academy also signposts parents to an annual Online Safety Workshop/information session, accessed through the Knowsley City Learning Centres website.**

Messages to the public around online safety should also be targeted towards grandparents and other adults engaging with pupils. Everyone has a role to play in empowering young people to stay safe while they enjoy these new technologies, just as it is everyone’s responsibility to keep them safe in the non-digital world.

Acceptable Use Agreement – pupil (KS1)

This is how we stay safe when we use computers:

- I will ask an adult if I want to use the computer, Chrome Book or I Pad
- I will only use activities/Apps if an adult says it is OK.
- I will take care of the computer and other equipment
- I will ask for help from an adult if I am not sure what to do or if I think I have done something wrong.
- I will turn off the monitor and tell an adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer or other equipment.

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

My name:	
Signed (child):	
OR Parent's signature:	
Date:	

Acceptable Use Agreement – pupil (KS2)

I understand that while I am a member of Tenbury Primary Academy I must use technology in a responsible way.

For my own personal safety:

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

For the safety of others:

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

For the safety of the school/academy:

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

KS2 Pupil Acceptable Use Agreement Form

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

Name:	
Signed:	
Date:	

Acceptable Use Agreement – staff & volunteer

Background

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.

I understand that I must use academy 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.

For my professional and personal safety:

- I understand that the school/academy will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of academy ICT systems (e.g. laptops, email,) out of the academy.
- I understand that the academy ICT 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 down in the online safety policy.
- 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 immediately report any illegal, inappropriate or harmful material or incident of which I become aware, to the appropriate person.

I will be professional in my communications and actions when using academy ICT 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 academy's policy on the use of digital images. I will not use my personal equipment to record these images.
- Where images are published (e.g. on the academy website) I will ensure that 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 academy's policies.
- I will only communicate with pupils and parents / carers using official academy systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The academy *and the local authority* have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the academy:

- I will only use my personal mobile ICT devices as agreed in the online safety policy and then with the same care as if I was using school/academy equipment. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the academy ICT systems other than exceptional school-related circumstances.
- 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 academy policies (Maintained and subscribing establishments see **IBS Schools Systems and Data Security advice**).

- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist or radical 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 academy policies.
- I will not disable or cause any damage to academy equipment, or the equipment belonging to others.
- I will not take or access pupil data, or other sensitive academy data, off-site without specific approval. If approved to do so, I will take every precaution to ensure the security of the data,
- 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 academy policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

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
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of academy:

- I understand that this Acceptable Use Agreement applies not only to my work and use of academy ICT equipment in the academy, but also applies to my use of academy ICT systems and equipment out of the academy and to my use of personal equipment in the academy or in situations related to my employment by the academy.
- I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action. This could involve a warning, a suspension, referral to Governors and/or the Local Authority and/or other relevant bodies including, in the event of illegal activities, the involvement of the police

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

Staff / volunteer Name:	
Signed:	
Date:	

Acceptable Use Agreement and permission forms – parent / carer

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 Acceptable Use Agreement is intended to ensure that:

- young people will be responsible users and stay safe while using ICT (especially the internet).
- school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- parents and 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.

The academy 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.

Parents are requested to sign the permission form below to show their support of the academy in this important aspect of their work.

Child's name	
Parent's name and signature	
Date:	

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 the academy.

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 and responsible use of ICT – both in and out of the academy.

I understand that the academy will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school/academy 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 ICT systems will be monitored and that the academy will contact me if they have concerns about any possible breaches of the Acceptable Use Agreement.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the academy if I have concerns over my child's online safety.

Parent's signature:	
Date:	

Permission to use digital images (still and video) of my child

The use of digital images (still and video) plays an important part in learning activities. Pupils and members of staff may use the academy's digital cameras and I Pads to record evidence of activities in lessons and on school trips. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the academy website and occasionally in the public media.

The academy will comply with the Data Protection Act and request parents / carers permission before taking images of members of the academy. The academy will also ensure that when images are published, the young people cannot be identified by name.

As the parent/carer of the above pupil, I agree to the academy taking and using digital images of my child(ren). I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the academy.

I agree that if I take digital or video images at academy events which include images of children, I will abide by these guidelines in my use of these images. I agree that I will not post such images of children, other than my own, on social networking sites.

Parent's signature:	
Date:	

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

It is our academy's policy, from time to time, to publish the work of pupils by way of celebration. This includes on the internet; via the website.

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

Parent's signature:	
Date:	

Permission to for my child to participate in video-conferencing

Videoconferencing technology is used by the academy in a range of ways to enhance learning – for example, by linking to an external "expert", or to an overseas educational partner. Video conferencing only takes place under teacher-supervision. Independent pupil use of video-conferencing is not allowed.

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

Parent's signature:	
Date:	

Guidance for Reviewing Internet Sites

This guidance is intended for use when the school/academy 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.

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 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. *This will automatically be done for you if you are using Policy Central from Forensic Software or other monitoring software.* 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 group 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 of 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.

A sample document for recording the review of and action arriving from the review of potentially harmful websites can be found on the next page

Group	
Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

Name and location of computer used for review (for web sites)

Web site(s) address / device	Reason for concern

Conclusion and Action proposed or taken

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 are contact details for further information and questions concerning the site's information and content.
- The site contains appropriate endorsements by external bodies and/or links to/from well-trusted sources

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

- The content is age-appropriate
- The content is broadly balanced in nature, and does not appear unduly biased, partisan or unreliable
- 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**
- The content of the website is current.

C. 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?

D. ACCESSIBILITY - Is the website accessible?

- Does it load quickly?
- Does the site require registration or passwords to access it?
- Is the site free from subscription charges or usage fees?

Supporting resources and links

The following links may help those who are developing or reviewing a academy online safety policy.

General

South West Grid for Learning "SWGfL Safe" - http://www.swgfl.org.uk/Staying-Safe

Child Exploitation and Online Protection Centre (CEOP) http://ceop.police.uk/

ThinkUKnow http://www.thinkuknow.co.uk/

ChildNet http://www.childnet.com/

InSafe http://www.saferinternet.org/

Byron Reviews ("Safer Children in a Digital World") - https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis

Becta – various useful resources now archived http://webarchive.nationalarchives.gov.uk/20101102103654/http:/www.becta.org.uk

London Grid for Learning - http://www.lgfl.net/esafety/Pages/education.aspx?click-source=nav-esafety

Northern Grid - http://www.digitallyconfident.org

National Education Network - http://www.nen.gov.uk/online safety/

WMNet – http://www.wmnet.org.uk

EU kids Online - http://www.lse.ac.uk/media%40lse/research/EUKidsOnline/Home.aspx

Cyber Bullying

Teachernet "Safe to Learn – embedding anti-bullying work in schools" (Archived resources)

http://tna.europarchive.org/20080108001302/http://www.teachernet.gov.uk/wholeschool/academy/behaviour/tacklingbullying/cyberbullying/

Anti-Bullying Network - http://www.antibullying.net/cyberbullying1.htm

Cyberbullying.org - http://www.cyberbullying.org/

CyberMentors: young people helping and supporting each other online - http://www.cybermentors.org.uk/

Prevent Duty - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/439598/prevent-duty-departmental-advice-v6.pdf

Social networking

Digizen – "Young People and Social Networking Services": http://www.digizen.org/socialnetworking/

Get Safe On-line - https://www.getsafeonline.org/social-networking

Connect Safely - Smart socialising: http://www.connectsafely.org/

Mobile technologies

"How mobile phones help learning in secondary schools":

http://archive.teachfind.com/becta/research.becta.org.uk/upload-dir/downloads/page_documents/research/lsri_report.pdf

"Guidelines on misuse of camera and video phones in school/academies"
http://www.dundeecity.gov.uk/dundeecity/uploaded_publications/publication_1201.pdf

Data protection and information handling

Information Commissioners Office - Data Protection:

http://www.ico.gov.uk/Home/what_we_cover/data_protection.aspx

Digital Parenting - http://www.vodaphone.com/parents

http://www.digitalparenting.ie/

https://www.commonsensemedia.org/

Links to other resource providers

SWGfL has produced a wide range of information leaflets and teaching resources, including films and video clips – for parents and school/academy staff. A comprehensive list of these resources (and those available from other organisations) is available on the "SWGfL Safe" website: http://www.swgfl.org.uk/staying-safe

BBC Webwise: http://www.bbc.co.uk/webwise/

Kidsmart: http://www.kidsmart.org.uk/default.aspx

Know It All - http://www.childnet-int.org/kia/

Cybersmart - http://www.cybersmartcurriculum.org/home/

Internet Watch Foundation: http://www.iwf.org.uk

Digizen – cyber-bullying films: http://old.digizen.org/cyberbullying/film.aspx

Glossary of terms

AUA	Acceptable Use Agreement
Becta	British Educational Communications and Technology Agency (former government agency which promoted the use of information and communications technology – materials and resources are archived and still relevant)
CEOP	Child Exploitation and Online Protection Centre (part of UK Police), dedicated to protecting children from sexual abuse. Providers of the Think U Know programmes.
DfE	Department for Education
FOSI	Family Online Safety Institute
ICT	Information and Communications Technology
ICT Mark	Quality standard for school/academys provided by NAACE for DfE
INSET	In-service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
IWF	Internet Watch Foundation
JANET	Provides the broadband backbone structure for Higher Education and for the National Education Network and Regional Broadband Consortia
KS1; KS2	KS1 = years 1 and 2 (ages 5 to 7) KS2 = years 2 to 6 (age 7 to 11)
LA	Local Authority
LAN	Local Area Network
Learning platform	An online system designed to support teaching and learning in an educational setting
LSCB	Local Safeguarding Children Board
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (eg WMNet) to provide the safe broadband provision to school/academys across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
Ofsted	Office for Standards in Education, Children's Services and Skills
PDA	Personal Digital Assistant (handheld device)
PHSE	Personal, Health and Social Education
SRF	Self Review Framework – a tool maintained by Naace used by school/academies to evaluate the quality of their ICT provision and judge their readiness for submission for the ICTMark
SWGfL	South West Grid for Learning – the Regional Broadband Consortium of SW Local Authorities and recognised authority on all matters relating to online safety (on whose policy this one is based)
URL	Universal Resource Locator – a web address

WMNet	The Regional Broadband Consortium of West Midland Local Authorities – provides support for all school/academys in the region and connects them all to the National Education Network (Internet)
WSCB	Worcestershire Safeguarding Children Board (the local safeguarding board)

Template Reporting Log

Reporting Log

Group .....

Date	Time	Incident	Action taken		Incident Reported by	Signature
			What?	By whom?		

Consent Form for use of Images (photographs, videos, DVDs and digital images)

Photographs and/or video recordings of children may be taken whilst they attend the setting to celebrate their achievements and successes and as evidence of their progress and development. Still or moving images may be published in our printed publications (e.g. prospectus, newsletters) and/or on our external websites. They may also be used to promote the good practice of the setting to other teachers, e.g. at training events organised by the Local Authority or national education/government institutions. Children's names will never be published alongside their photograph externally to the education setting. Names may be used internally, for example – on a display.

Electronic images, whether photographs or videos, will be stored securely on the setting's network which is accessible only by authorised users.

Before using any photographs/videos of your child we need your permission. **Please answer the questions below, then sign and date the form where indicated and return it.**

Please circle

1. May we use your child's photograph in printed publications? **Yes / No**

2. May we use your child's photograph on our internet websites? **Yes/No**

3. May we allow your child's photograph (e.g. as part of a team or record of an event) to be used for publication in a newspaper? **Yes / No**

   (Please note that the use of photographs in newspapers is subject to strict guidelines)

4. May we use any photograph or video of your child internally as part of regular activities and work of the setting? **Yes / No**

5. May we use any photographs or video containing your child to share good practice with staff from other settings? **Yes / No**

6. May we use images of your child on an external web site or for publicity or campaigns by national Government agencies?

   Yes/No

7. May we use examples of your child's work and publish it from time to time on the internet via the website or in the local newspaper. The full name of the child will not be published **Yes/ No**

This form is valid from the date of signing until your child leaves the setting. Photographs and videos may be securely archived after your child has left the setting. Photographs and videos used for publicity purposes may continue to remain in circulation after your child has left the setting. You may withdraw your consent, in writing, at any time **but it may not be possible to remove images that are already in circulation or have already been published** although every effort will be made to do so.

We recognise that parents, carers and family members will wish to record events such as plays, sports days etc. to celebrate their child's achievements. The setting is happy to allow this, at the discretion of the Headteacher/Senior Manager, on the understanding that such images/recordings are used for purely personal family use. Images containing children **other than their own** should not be put on the internet for any reason, without first seeking permission from the other child's parents/carers.

A full copy of the setting's policy on the safe use of children's photographs may be obtained upon request.

Name of Child: …… Date of birth: ……

Name of person with Parental Responsibility: ……

Signed: …… Date: ……

Data Protection

Tenbury CE Primary Academy takes your privacy seriously and we have taken steps to protect it. Any personal data you give to us, including photographic images, will be processed strictly in accordance with the Data Protection Act 1998 and will be used for the purposes that you have consented to. We will not share your details with third parties without your consent, except where we are legally compelled or obligated to do so. Please note that where you consent to images appearing on the internet, they can be viewed worldwide including countries where UK data protection law does not apply.

Social Networking Teacher Agreement

For the protection of yourself, your school community and your establishment:

- Ensure that all your privacy settings are set to 'Friends Only'. Go to your Account Settings and make sure that the Custom Settings are highlighted and that these show that status, photos and posts are set to 'Friends Only'.
- Consider what information you have on your info page and your profile picture. Including brief information and an unidentifiable picture, e.g. sunset, will assist in making your profile indistinctive.
- Be careful what photographs you include on your profile. Once these are uploaded, they are very difficult to remove and, using image editing software, they can be altered and merged with other more distasteful images.
- If you have professional and social 'friends' on Facebook or other social networking sites, using the group list feature will ensure that you can distinguish what type of information you send to particular groups.
- Do not accept pupils (even those that have recently left the school)
- If you choose to accept parents/carers as 'friends' a different identity will be used.
- Do not use Facebook or other social networking sites in any way that might bring your professional status or your school into disrepute.
- Taking charge of your digital reputation is important, as unprofessional posts or images will lead to disciplinary action and possible failure to gain employment in the future.
- Do not post or upload photographs relating to colleagues, pupils or parents. Objection to such posts can cause friction in your school and make your working environment uncomfortable.
- Do not post or upload photographs related to school-based or extra-curricular activities and do not make specific reference to your school in any post as comments may be misconstrued and result in inappropriate responses.
- Be aware of any spam or potential virus risks sent via rogue posts. It is advisable to check with anti-virus firms if you get any suspicious requests or posts.
- If you are alerted to any negative or unscrupulous information about yourself, colleagues or your school on Facebook or other social networking sites, inform your headteacher. Further advice to help with cyberbullying incidents etc., can be gained from help@saferinternet.org.uk (0844 3814772) or a professional association such as your Trade Union.
- ***I understand the implications of using Facebook and other social networking sites for my own protection and professional reputation, as well as the impact that my use can have on my school community and establishment.***

- ***I understand that injudicious use of social networking may lead to disciplinary action.***
- ***I agree to take all possible precautions as outlined above.***

Name		***Date***	