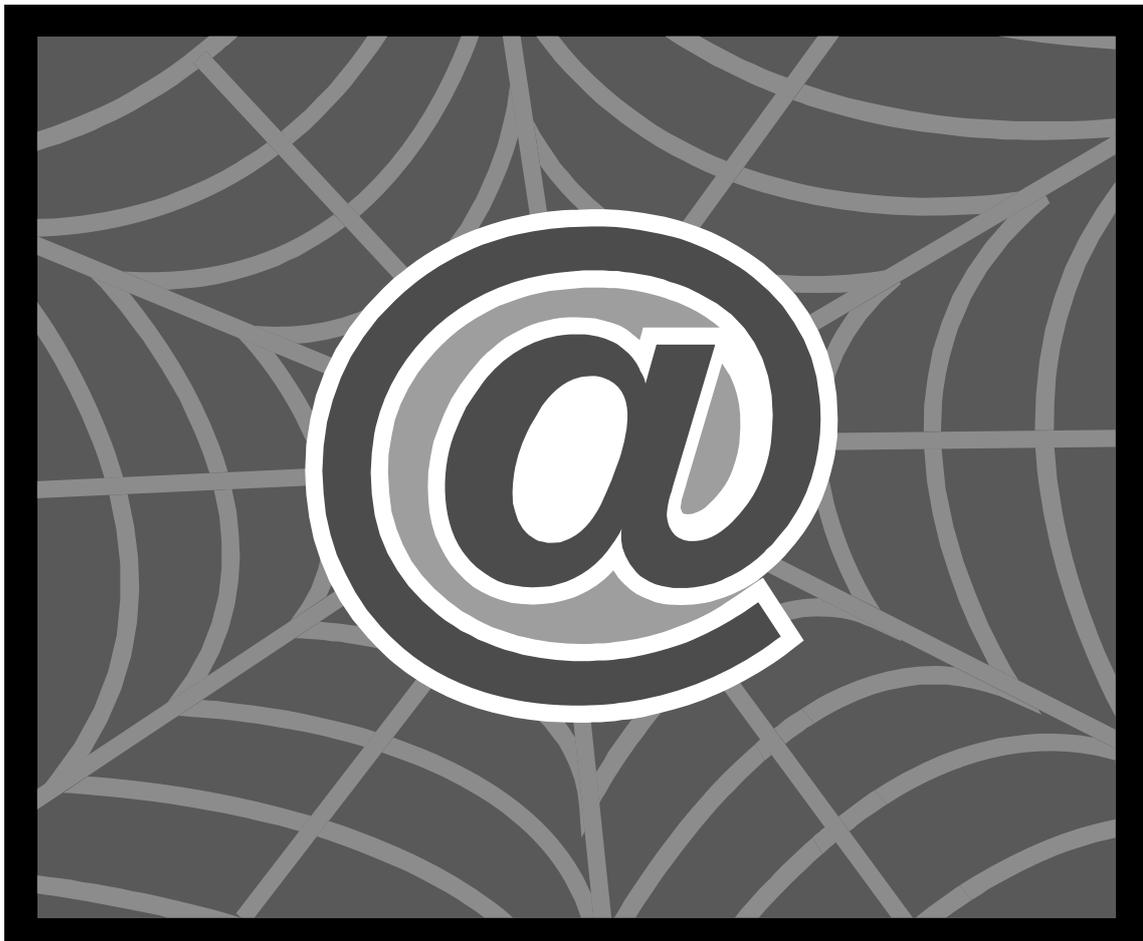


Worcestershire Children's Services

# On-line Safety Policy for Worcestershire Schools

Tenacres First School May 2017



This policy is based on a template from the South West Grid for Learning available at:

<http://www.swgfl.org.uk/Staying-Safe/Content/News-Articles/Creating-an-online-safety-policy--Where-do-you-start->

This revision for Worcestershire took place in Autumn 2014

# 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 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.”*

Schools/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 (see September 2013 Section 5 OFSTED briefings). Many schools/academies are opting to gain recognition for the quality of their ICT provision through ICTMark accreditation. The ICTMark Self Review Framework (SRF) contains a number of aspects regarding the school’s online safety policies and provision.

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 and in lessons
- how well the school 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

- **KS3:** understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy; recognise inappropriate content, contact and conduct and know how to report concerns.
- **KS4:** understand how changes in technology affect safety, including new ways to protect their online privacy and identity, and how to report concerns.

# Contents

Introduction.....	2
Behaviour and safety of pupils at the school.....	2
Contents.....	4
Background and rationale .....	6
Section A - Policy and leadership .....	7
A.1.1    Responsibilities: the online safety committee .....	7
A.1.2    Responsibilities: online safety coordinator – Jon Beacham.....	7
A.1.3    Responsibilities: governors .....	7
A.1.4    Responsibilities: head teacher.....	8
A.1.5    Responsibilities: classroom based staff.....	8
A.1.6    Responsibilities: ICT technician - Arrow Vale Technicians – Ash Burbridge / Dan Carpenter.....	8
A.2.1    Policy development, monitoring and review .....	9
Schedule for development / monitoring / review of this policy.....	10
A.2.2    Policy Scope.....	10
A.2.3    Acceptable Use Agreements .....	11
A.2.4    Self Evaluation .....	11
A.2.5    Whole School approach and links to other policies.....	11
Core ICT policies .....	11
Other policies relating to online safety .....	12
A.2.6    Illegal or inappropriate activities and related sanctions.....	12
A.3.1    Use of hand held technology (personal phones and other hand held devices).....	16
A.3.2    Use of communication technologies.....	18
A.3.2a - Email.....	18
A.3.2b - Social networking (including chat, instant messaging, blogging etc) .....	19
A.3.3    Use of digital and video images .....	19
A.3.4 - Website (and other public facing communications).....	19
A.3.4b – Learning Platform .....	20
A.3.5    Professional standards for staff communication.....	20
Section B. Infrastructure .....	21
B.1    Password security .....	21
B.2.1    Filtering.....	21
B.2.2    Technical security.....	22
B.2.3    Personal data security (and transfer) .....	23
Section C. Education.....	23
C.1.1    Online safety education .....	23

C.1.2	Information literacy .....	23
C.1.3	The contribution of the pupils to the e-learning strategy .....	24
C.2	Staff training .....	24
C.3	Governor training.....	24
C.4	Parent and carer awareness raising.....	24
C.5	Wider community understanding.....	25
Appendix 1 – .....		26
Appendix 1a – Acceptable Use Agreement – pupil .....		26
Appendix 1b – Acceptable Use Agreement – staff & volunteer .....		27
Appendix 1d - Acceptable Use Agreement and permission forms – parent / carer.....		<b>Error!</b>
<b>Bookmark not defined.</b>		
Appendix 1e - Acceptable Use Agreement – community user .....		29
Appendix 2 - Guidance for Reviewing Internet Sites.....		30
Appendix 3 – Criteria for website filtering .....		32
Appendix 4 - Supporting resources and links.....		33
Appendix 5 - Glossary of terms .....		35
Appendix 6 Reporting Log.....		37
Appendix 7 Guidance to support the safe and appropriate use of images in schools and settings .....		38
Appendix 8 Social Networking Teacher Agreement.....		43
Appendix 9 Loaned Device User Agreement .....		44

# 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 environment (parents, friends and the wider community) to be aware and to assist in this process.

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

# Section A - Policy and leadership

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

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

## A.1.1 Responsibilities: the online safety committee

Our school has an online safety committee lead by our online safety and safeguarding coordinator and made up of our Digital Leaders, teachers, our school bursar and our online safety and parent governor. It meets on a termly basis to:

- Review and monitor this online safety policy.
- Consider any issues relating to school filtering (see section B.2.1 of this policy)
- Discuss any online safety issues that have arisen and how they should be dealt with.

Issues that arise are referred to other school bodies as appropriate and, when necessary, to bodies outside the establishment, such as the Worcestershire Safeguarding Children Board.

## A.1.2 Responsibilities: online safety coordinator – Jon Beacham

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:

- leads the online safety committee
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school 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
- liaises with school 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 each half term 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

## A.1.3 Responsibilities: governors

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

- regular meetings with the Online safety Co-ordinator each half term with an agenda based on:
  - monitoring of online safety incident logs
  - reporting to relevant Governors committee / meeting

### **A.1.4 Responsibilities: head teacher**

- The head teacher is responsible for ensuring the safety (including online safety) of all members of the school community, though the day to day responsibility for online safety is delegated to the Online safety Co-ordinator
- The head teacher and another member of the senior management team will be familiar with the procedures to be followed in the event of a serious online safety allegation being made against a member of staff, including non-teaching staff. (see flow chart on dealing with online safety incidents (included in section 2.6 below) and other relevant Local Authority / HR disciplinary procedures)

### **A.1.5 Responsibilities: classroom based staff**

Teaching and Support Staff are responsible for ensuring that:

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

### **A.1.6 Responsibilities: ICT technician - Arrow Vale Technicians – Ash Burbridge / Dan Carpenter**

The ICT Technician is responsible for ensuring that:

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

## **A.2.1 Policy development, monitoring and review**

This online safety policy has been developed (from a template provided by Worcestershire County Council) by a working group made up of:

- Online safety Coordinator
- Safeguarding officer
- Head teacher
- Teachers
- Governors (especially the online safety governor)
- Parents
- Pupils

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

- Staff meetings
- Digital Leader meetings
- INSET Training for Teachers, TAs and Lunchtime Supervisors
- Governor's meeting / subcommittee meeting
- School website & blog / newsletters

## Schedule for development / monitoring / review of this policy

This online safety policy was approved by the governing body on:	Insert date
The implementation of this online safety policy will be monitored by the:	Headteacher / Safeguarding coordinator- Ceri Marshall Online safety coordinator – Jon Beacham School bursar – Michaela Carpenter Parent governor – Steph Mann Online Safety / Safeguarding Governor – Anita Clayton Digital Leaders – Tegan, Stan, Luca and Molly
Monitoring of this policy will take place at regular intervals:	Once a year
The governing body will receive regular reports on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) as part of a standing agenda item with reference to safeguarding:	Once a year
The online safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of technology, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	April 2018
Should serious online safety incidents take place, the following external persons / agencies should be informed:	Worcestershire Safeguarding Children Board Local Authority Designated Officer Worcestershire Senior Adviser for Safeguarding Children in Education West Mercia Police

### A.2.2 Policy Scope

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

The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, radicalisation or other online safety incidents covered by this policy, which may take place out of the school, but are linked to membership of the school.

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

### **A.2.3 Acceptable Use Agreements**

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

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

- Pupils (adapted terminology and length – signed each year. Displayed in front of Home School Diary)
- Staff (and volunteers)
- Parents / carers
- Community users of the school’s ICT system
- Technical support personnel

Acceptable Use Agreements are introduced at parents’ induction meetings and signed by all parents and pupils as they enter school.

Pupils re-sign each year.

All employees of the school 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 school. The parents’ policy also includes permission for use of their child’s image (still or moving) by the school, permission for their child to use the school’s ICT resources (including the internet) and permission to publish their work.

Community users sign when they first request access to the school’s ICT system.

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

### **A.2.4 Self Evaluation**

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

### **A.2.5 Whole School approach and links to other policies**

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

#### **Core ICT policies**

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

Computing curriculum and/or Worcestershire Primary ICT Progressions

Key documents and associated resources directly relating to learning covering the Computing Curriculum

## Other policies relating to online safety

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

### A.2.6 Illegal or inappropriate activities and related sanctions

The school 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 school equipment or systems (**in or out of school**).

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

- **child sexual abuse images (illegal - The Protection of Children Act 1978)**
- **grooming, incitement, arrangement or facilitation of sexual acts against children (illegal – Sexual Offences Act 2003)**
- **possession of extreme pornographic images (illegal – Criminal Justice and Immigration Act 2008)**
- **criminally racist material in UK – to stir up religious hatred 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 or brings the school into disrepute

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

- Using school systems to undertake transactions pertaining to a private business
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Worcestershire County Council Broadband 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)
- On-line gambling and non-educational gaming
- On-line shopping / commerce unless directly related to school business
- Use of social networking sites (other than in the school's learning platform or sites otherwise permitted by the school)

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 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 indicated on the following pages:

## Pupil sanctions

The indication of possible sanctions in this table should not be regarded as absolute. They should be applied according to the context of any incident and in light of consequences from the offence.

	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
<b>Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).</b>	✓	✓	✓	✓	✓	✓	✓	✓	✓
Unauthorised use of non-educational sites during lessons	✓				✓				
Unauthorised use of mobile phone / digital camera / other handheld device	✓					✓	✓		
Unauthorised use of social networking / instant messaging / personal email	✓	✓			✓	✓		✓	
Unauthorised downloading or uploading of files	✓						✓	✓	
Allowing others to access school network by sharing username and passwords	✓	✓	✓		✓		✓	✓	
Attempting to access the school network, using another pupil's account	✓				✓		✓		
Attempting to access or accessing the school network, using the account of a member of staff	✓		✓		✓	✓		✓	
Corrupting or destroying the data of other users	✓		✓		✓	✓	✓	✓	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓	✓		✓	✓	✓	✓	
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 <b>and failing to report the incident</b>	✓	✓			✓	✓			
<b>Deliberately</b> 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

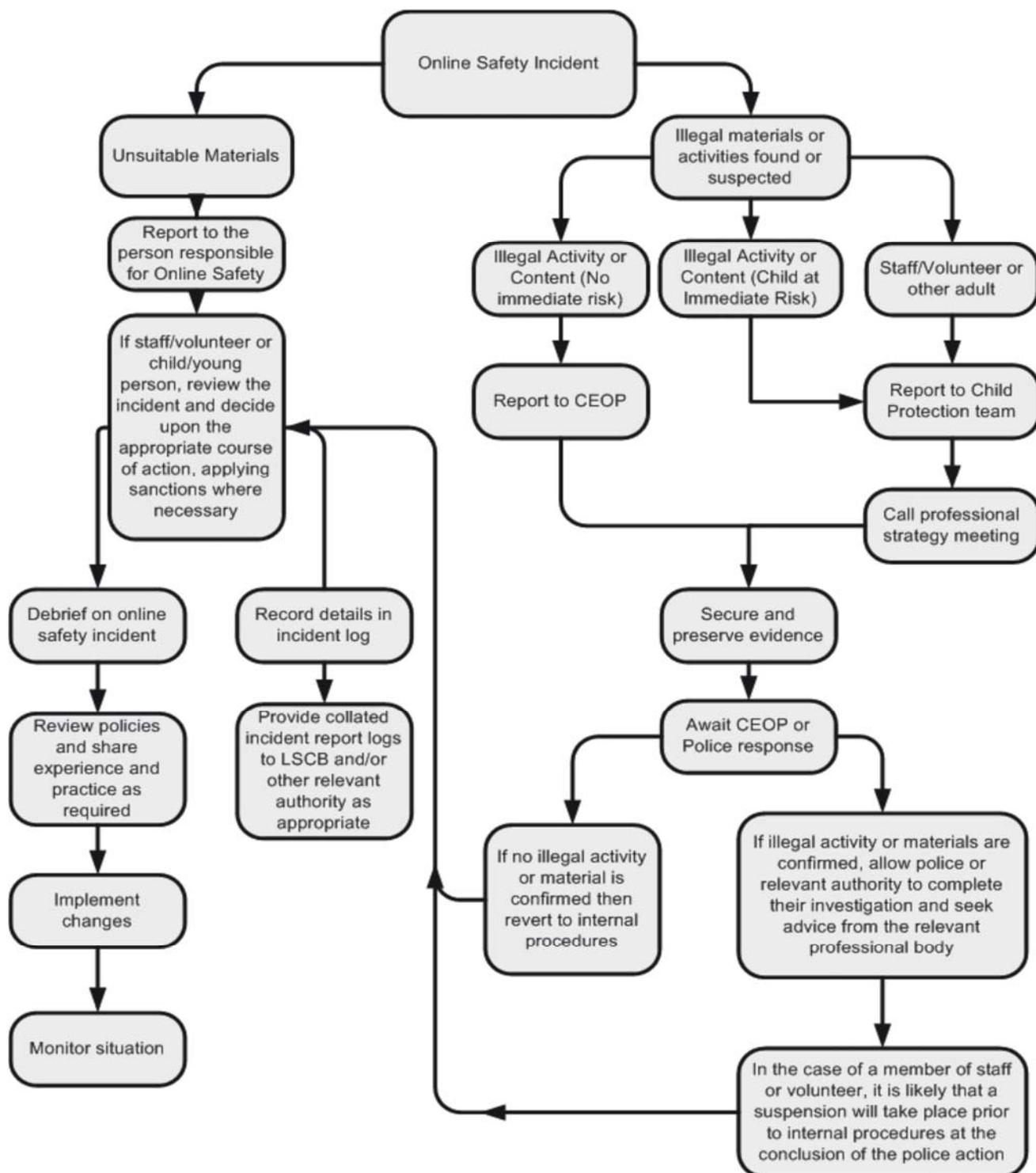
The indication of possible sanctions in this table should not be regarded as absolute. They should be applied according to the context of any incident and in the light of consequences resulting from the offence.

	Refer to:					Action:		
	Line manager	Head teacher	Local Authority / HR	Police	Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
<b>Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).</b>	✓	✓	✓	✓	✓		✓	✓
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 <b>and failing to report the incident</b>	✓	✓			✓	✓		
<b>Deliberately</b> accessing or trying to access offensive or pornographic material	✓	✓	✓		✓	✓	✓	✓
Breaching copyright or licensing regulations	✓					✓		
Continued infringements of the above, following previous warnings or sanctions	✓	✓			✓			✓

## A.2.7 Reporting of online safety breaches

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

Particular care should be taken if any apparent or actual misuse appears to involve illegal activity listed in section A.2.6 of this policy



## A.3.1 Use of hand held technology (personal phones and other hand held devices)

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

- Members of staff are permitted to bring their personal mobile devices into school. They are required to use their own professional judgement as to when it is appropriate to use them. Broadly speaking this is:
  - ✓ Personal hand held devices will be used in lesson time only in an emergency or extreme circumstances
  - ✓ Members of staff are free to use these devices outside teaching time.
  - ✓ A school mobile phone is available for all professional use (for example when engaging in off-site activities). Members of staff should **not** use their personal device for school purposes except in an emergency.
- Pupils are not currently permitted to bring their personal hand held devices into school.
- A number of such devices are available in school (e.g. iPads) and are used by pupils as considered appropriate by members of staff.

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

## A.3.2 Use of communication technologies

### A.3.2a - Email

As a school we use Office 365 including Outlook for our email system. This official school email services may be regarded as safe and secure and are monitored.

- Staff and pupils should use only the school email services to communicate with others regarding school business when in school, or on school systems (e.g. by remote access)
- Users need to be aware that email communications may be monitored
- Pupils normally use only an email account to communicate with people outside school 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 (see section C of this policy)
- **Staff may only access personal email accounts on school 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.

Use of Email	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 personal email accounts in school / on school network			↙					↙
Use of school email for personal emails				↙				↙

## A.3.2b - 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				✗				✗

## A.3.3 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. (See section C). 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 school equipment; **the personal equipment of staff should not be used for such purposes.**
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Staff should be aware of pupils for whom it has been deemed inappropriate to take and share/publish their photograph (e.g. some looked after children)
- Pupils must not take, use, share, publish or distribute images of others without their permission

See also the following section (A.3.4) for guidance on publication of photographs

## A.3.4 - Website (and other public facing communications)

Our school uses the public facing website [www.tenacres.worcs.sch.uk](http://www.tenacres.worcs.sch.uk) only for sharing information with the community beyond our school. This includes, from time-to-time, celebrating work and achievements of pupils. All users are required to consider good practice when publishing content.

- Personal information will not be posted on the school website and only official email addresses will be used to identify members of staff (never pupils).
- 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
  - ✓ written permission from parents or carers will be obtained before photographs of pupils are published on the school website (see section A.2.3 and Appendix 1)
- Pupil's work can only be published with the permission of the pupil and parents or carers. (see section A.2.3 and Appendix 1)

### **A.3.4b – Learning Platform**

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

Staff use is monitored by the super-user/administrator.

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

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

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

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

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

- a) The user will be asked to remove any material deemed to be inappropriate or offensive.
- b) The material will be removed by the site administrator if the user does not comply.
- c) Access to the learning platform may be suspended for the user.
- d) The user will need to discuss the issues with a member of SLT before reinstatement.
- e) A pupil's parent/carer may be informed.

A visitor may be invited onto the learning platform by the administrator following a request from a member of staff. In this instance there may be an agreed focus or a limited time slot / access.

### **A.3.5 Professional standards for staff communication**

In all aspects of their work in our establishment, teachers abide by the broad **Professional Standards for Teachers** laid down by the TDA effective from September 2012:

<http://media.education.gov.uk/assets/files/pdf/t/teachers%20standards.pdf>.

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

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

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

# Section B. Infrastructure

## B.1 Password security

This is dealt with in detail in our school's **E-security Policy**. Please refer to that document for more information.

The school's online safety curriculum will include frequent discussion of issues relating to password security and staying safe in and out of school (see section C of this policy)

## B.2.1 Filtering

### B.2.1a - Introduction

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

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

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

### B.2.1b - Responsibilities

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

To ensure that there is a system of checks and balances and to protect those responsible, changes to the standard Worcestershire, or other, school filtering service must:

- be logged in change-control logs by the person making the change
- be reported to, and authorised by, a second responsible person prior to changes being made

**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.

### B.2.1c - Education / training / awareness

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

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

- signing the Acceptable Use Agreement (as part of their induction process)
- briefing in staff meetings, training days, memos etc. (timely and ongoing).

**Parents** will be informed of the school's filtering policy through the Acceptable Use Agreement and through newsletters etc.

## **B.2.1d - Changes to the filtering system**

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

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

THEN If agreement is reached, the online safety coordinator makes a request to IBS Schools Broadband Team.

- The team will endeavour to unblock the site within 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.

The online safety coordinator will need to apply a rigorous policy for approving / rejecting filtering requests. This can be found in Appendix 3 but the core of 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.

## **B.2.1e - Monitoring**

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

Monitoring takes place as follows:

- At least 2 identified members of staff (members of SLT / online safety co-ordinator / safeguarding officer) review the monitoring console captures in turn, 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.

## **B.2.1f - Audit / reporting**

Filter change-control logs and incident logs are made available to:

- the online safety governor within the timeframe stated in section A.1.3 of this policy
- the online safety committee (see A.1.1)
- 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.

## **B.2.2 Technical security**

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

## **B.2.3 Personal data security (and transfer)**

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

Teachers frequently discuss issues relating to data security and how it relates to staying safe in and out of school (see section C of this policy)

# **Section C. Education**

## **C.1.1 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 school's online safety provision. Children and young people need constant help and support to recognise and avoid online safety risks and build their resilience. This is particularly important for helping them to 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 and other lessons. This is regularly revisited, covering the use of ICT and new technologies both in school and beyond school
- Key online safety messages will be reinforced through further input via assemblies and pastoral activities, as well as informal conversations when the opportunity arises.
- Pupils will be helped to understand the pupil Acceptable Use Agreement (see Appendix 1) and encouraged to adopt safe and responsible use of ICT both within and outside the school.
- 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 will be made aware of what to do should they experience anything, while on the Internet, which makes them feel uncomfortable.

## **C.1.2 Information literacy**

- Pupils should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information by employing techniques such as:
  - ✓ Checking the likely validity of the URL (web address)
  - ✓ Cross checking references (Can they find the same information on other sites?)
  - ✓ Checking the pedigree of the compilers / owners of the website
  - ✓ Referring to other (including non-digital) sources
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils are taught how to make best use of internet search engines to arrive at the information they require

- We use the resources on CEOP's Think U Know site as a basis for our online safety education <http://www.thinkuknow.co.uk/teachers/resources/>.

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

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

Pupils play a part in monitoring this policy (see section A.1.1)

## **C.2 Staff training**

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

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

## **C.3 Governor training**

**Governors should take part in 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), National Governors Association or other bodies.
- Participation in school training / information sessions for staff or parents

The online safety governor works closely with the online safety coordinator and reports back to the full governing body (see section A.1.3)

## **C.4 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 school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site

## **C.5 Wider community understanding**

The school will offer family learning courses in ICT, media literacy and online safety so that parents and pupils can together gain a better understanding of these issues.

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.

Community Users who access school ICT systems / website / learning platform as part of extended school provision will be expected to sign a Community User Acceptable Use Agreement (see Appendix 1) before being provided with access to school systems.

# Appendix 1 –

## Appendix 1a – Acceptable Use Agreement – pupil

### Online Safety guidelines

All pupils at Tenacres First School use computer facilities including Internet access as an essential part of learning. We have filtering, monitoring software and content control to minimise access to inappropriate content via the school network system.

Pupils are given information on Online Safety during PSHE lessons, assemblies and dedicated Computing lessons.

**E-mail:** Pupils may only use their approved class email accounts on the school network during designated teaching sessions. Teachers will always check the children's emails before they are sent.

**Please read the Online Safety rules with your child and then sign to show they have been understood and agreed by you and your child.**

- We only use the internet if an adult or grown says we can. 
- We can click on the buttons or links if we think they are safe. 
- We can ask to use the internet in lessons for research. 
- We always ask if we get lost on the Internet. 
- We can send and open friendly emails together only to people we know. 
- We only search for pictures and videos that we need for schoolwork. 
- If we see something that upsets us, we follow these simple steps: turn the screen off, tell an adult and never share or go back!

### Consent for Internet Access:

I have read and understood the school e-safety rules and give permission for my child to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

(parent) Signed: \_\_\_\_\_ Date: \_\_\_\_\_

(child) Signed: \_\_\_\_\_ Date: \_\_\_\_\_

### Social Networking

We trust that you recognise the dangers of discussing school issues on social networking sites and stress the importance of parents/carers supporting the school and raising any concerns directly with us.

# Appendix 1b – 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 school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I will, where possible, educate the young people in my care in the safe use of ICT and embed online safety in my work with young people.

### For my professional and personal safety:

- I understand that the school 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 school ICT systems (e.g. laptops, email, learning platform) out of the school.
- I understand that the school 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 school 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 school'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 school website / learning platform) I will ensure that it will not be possible to identify by name, or other personal information, those who are featured. (see section A.3.3 of the online safety policy)
- I will only use chat and social networking sites in school in accordance with the school's policies. (see section A.3.2 of the online safety policy)
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner. (see sections A.3.1 and A.3.2 of the online safety policy)
- I will not engage in any on-line activity that may compromise my professional responsibilities.

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

- I will only use my personal mobile ICT devices as agreed in the online safety policy (see section A.3.1) and then with the same care as if I was using school equipment. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems except in an emergency (A.3.2).
- 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 school 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 school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy (see e-security policy). **I understand that where personal data is transferred outside the secure school network, it must be encrypted.**
- I will not take or access pupil data, or other sensitive school 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 school 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 school:**

- I understand that this Acceptable Use Agreement applies not only to my work and use of school ICT equipment in the school, but also applies to my use of school ICT systems and equipment out of the school and to my use of personal equipment in the school or in situations related to my employment by the school.
- 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 (see section A.2.6).

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

Staff / volunteer Name:	
Signed:	
Date:	

## Appendix 1c - Acceptable Use Agreement – community user

You have asked to make use of our school's ICT facilities. Before we can give you a log-in to our system we need you to formally agree to use the equipment and infrastructure responsibly.

### For my professional and/or personal safety:

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

### I will be responsible in my communications and actions when using the school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files or data, 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.

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

- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist 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 described above.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, except with the specific approval of the school.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

**I have read and understand the above and agree to use the school ICT systems (both in and out of the school) within these guidelines. I understand that failure to comply with this agreement will result in my access to the school's ICT systems being withdrawn, that further actions will be taken in the event illegal activity, and that I may be held liable for any damage, loss or cost to the school as a direct result of my actions.**

Community user Name:	
Signed:	
Date:	

## Appendix 2 - Guidance for Reviewing Internet Sites

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

**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

**Record of reviewing devices / internet sites (responding to incidents of misuse)**

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**


# Appendix 3 – 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?

## Appendix 4 - Supporting resources and links

The following links may help those who are developing or reviewing a school 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/](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/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](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](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.dundee.gov.uk/dundee/uploaded\\_publications/publication\\_1201.pdf](http://www.dundee.gov.uk/dundee/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](http://www.ico.gov.uk/Home/what_we_cover/data_protection.aspx)

Digital Parenting - <http://www.vodafone.com/parents>

<http://www.digitalparenting.ie/>

<https://www.common sense media.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 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>

## Appendix 5 - Glossary of terms

<b>AUA</b>	Acceptable Use Agreement – see templates earlier in this document
<b>Becta</b>	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)
<b>CEOP</b>	Child Exploitation and Online Protection Centre (part of UK Police), dedicated to protecting children from sexual abuse. Providers of the Think U Know programmes.
<b>DfE</b>	Department for Education
<b>FOSI</b>	Family Online Safety Institute
<b>ICT</b>	Information and Communications Technology
<b>ICT Mark</b>	Quality standard for schools provided by NAACE for DfE
<b>INSET</b>	In-service Education and Training
<b>IP address</b>	The label that identifies each computer to other computers using the IP (internet protocol)
<b>ISP</b>	Internet Service Provider
<b>IWF</b>	Internet Watch Foundation
<b>JANET</b>	Provides the broadband backbone structure for Higher Education and for the National Education Network and Regional Broadband Consortia
<b>KS1; KS2</b>	KS1 = years 1 and 2 (ages 5 to 7) KS2 = years 2 to 6 (age 7 to 11)
<b>LA</b>	Local Authority
<b>LAN</b>	Local Area Network
<b>Learning platform</b>	An online system designed to support teaching and learning in an educational setting
<b>LSCB</b>	Local Safeguarding Children Board
<b>MIS</b>	Management Information System
<b>NEN</b>	National Education Network – works with the Regional Broadband Consortia (eg WMNet) to provide the safe broadband provision to schools across Britain.
<b>Ofcom</b>	Office of Communications (Independent communications sector regulator)
<b>Ofsted</b>	Office for Standards in Education, Children’s Services and Skills
<b>PDA</b>	Personal Digital Assistant (handheld device)
<b>PHSE</b>	Personal, Health and Social Education
<b>SRF</b>	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
<b>SWGfL</b>	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)
<b>URL</b>	Universal Resource Locator – a web address

**WMNet** The Regional Broadband Consortium of West Midland Local Authorities – provides support for all schools in the region and connects them all to the National Education Network (Internet)

**WSCB** Worcestershire Safeguarding Children Board (the local safeguarding board)

# Appendix 6 Reporting Log

Reporting Log							Signature
Group .....							
Date	Time	Incident	Action taken		Incident Reported by		
			What?	By whom?			

# Appendix 7 Guidance to support the safe and appropriate use of images in schools and settings

Based on:

Safeguarding Children and Safer Recruitment in Education – *Consultation version 2010*

Guidance for Safer Working Practice for Adults who work with Children and Young People in Education Settings – *DCSF March 2009*

Data Protection Good Practice Note: Taking Photographs in School – *Information Commissioner's Office 26<sup>th</sup> October 2007*

## Document Details:

Status: Final

Date: December 2011

Reviewed: December 2013

## Contacts:

Sally Mills, Senior Advisor, Safeguarding Children in Education [SMills@worcestershire.gov.uk](mailto:SMills@worcestershire.gov.uk)

Cath Ellicott, Early Years and Childcare Manager

[CEllicott@worcestershire.gov.uk](mailto:CEllicott@worcestershire.gov.uk),

## Introduction

There are many occasions when staff and parents will want to take photographs of children. Such occasions include everything from observation, evidence, assessment and curricular purposes in the classroom to award ceremonies, performances, trips and sporting events as part of the extended activities programme. The intention of this policy is to set out clear guidelines which will balance the use of photography as a source of pleasure and pride with the need to safeguard children and protect the rights of the individual.

The photography policy sets out to ensure that:

- Photographs are only used for the purpose intended
- Settings use of photographs is facilitated
- Personal family photography is allowed where possible
- Individual rights are respected and child protection issues considered
- Parents/carers and children are given the right to opt out.

## Definitions

The term 'images' refers to photographic prints or slides, digital images, videos or moving images. Images may be distributed via print, DVDs, the internet or other technologies.

The term ' settings' refers to Early Years Settings, Maintained Schools, Independent Schools, Free Schools, Academies, Short Stay Schools, Colleges of Further Education, out of school provision, childminders and Children's Centres.

## **Safeguarding Children**

The welfare and protection of our children is paramount and consideration should always be given to whether the use of photography will place our children at risk. Images may be used to harm children, for example as a preliminary to 'grooming' or by displaying them inappropriately on the internet, particularly social networking sites.

For this reason consent is always sought when photographing children and additional consideration given to photographing vulnerable children, particularly Looked After Children or those in domestic abuse situations. Consent must be sought from those with parental responsibility (this may include the Local Authority in the case of Looked After Children).

## **Data Protection**

The Information Commissioner's Office (ICO) maintains a public register which includes the name and address of 'data controllers' and details about the types of personal information they process. 'Notification' is the process by which each data controller's details are added to the register. All settings need to ensure they are registered with the Information Commissioner's Office every year. Failure to notify the ICO is a criminal offence. Notification is necessary if settings are processing personal information. This includes taking photographs of the children using a digital camera. Personal data (including photos) held by settings must be included in the setting's notification. Further information on data protection as well as details on how to notify can be found at:[http://www.ico.gov.uk/for\\_organisations/data\\_protection/notification.aspx](http://www.ico.gov.uk/for_organisations/data_protection/notification.aspx)

In October 2007, the Information Commissioner's Office issued the following advice:

*"The Data Protection Act is unlikely to apply in many cases where photographs are taken in schools and other educational institutions. Fear of breaching the provisions of the Act should not be wrongly used to stop people taking photographs or videos which provide many with much pleasure. Where the Act does apply, a common sense approach suggests that if the photographer asks for permission to take a photograph, this will usually be enough to ensure compliance.*

- *Photos taken for official school use may be covered by the act and pupils and students should be advised why they are being taken.*
- *Photos taken purely for personal use are exempt from the Act."*

**Please note that although notification is mandatory in most cases the data protection guidance within this document is 'recommended guidance' and settings must take individual responsibility for their own data protection issues in accordance with the Data Protection Act 1998.**

## **Parental Consent**

On admission of a child to a setting, parents/carers will be asked to complete a consent form indicating their agreement or objection regarding the use of images of their child. Consent should be discussed with the child, once they are old enough to understand, and the child also asked to sign the consent form. Parents/children should be asked to complete the separate WCC consent form for images that have been taken for the purpose of LA publicity.

A list of children for whom consent has been refused will be maintained by the setting and every effort will be made by staff not to include these children in photographs or video footage. The list will be updated on a regular basis<sup>1</sup>.

The parent/carer should be asked to confirm, in writing, that they will inform the setting if they no longer wish images of their child to be used for any reason. They need to be made aware that once images are in circulation or have been published, it may be impossible to remove them, although every effort will be made to ensure they are not used in future publications.

### **Setting Photography**

Photographic and/or video images taken by staff may be used for curricular and/or extra-curricular activities, displays, on the setting website, in the setting prospectus or newsletter, as evidence of the child's development or as part of publicity in the media. Staff will ensure that:

- They are clear about the purpose of the activity and what will happen to the images when the activity is concluded.
- They always use setting equipment for taking images.
- They never record images using their personal camera, mobile phone or video equipment or for their own personal use.
- They will never photograph children in a state of undress, for example whilst changing for PE or a performance.
- They will report any concerns about inappropriate or intrusive photographs found to the Senior Designated Person following the setting's safeguarding procedures
- They have parental permission to take; store and/or display the images.
- Childminding settings should pay particular attention to the safe storage of digital imagery if using their personal equipment to record and store images

### **Storage of Images**

Photographs retained in a setting will not be used other than for their original purpose, unless permission is obtained from the subject.

Images should always be stored securely and password protected.

Photographs should be destroyed or deleted from databases once they are no longer required for the purpose for which they were taken. Photographs taken for publicity and promotional purposes should be retained for a maximum of two years. Photographs contributing to the history of the setting, its children, activities or the community, may be retained indefinitely.

For schools, further information on storage and security can be found in the LA guidance *Schools System and Data Security*.

### **Parental Photography**

In many cases, photographs taken at setting events form an important part of family albums. Everything possible will be done to ensure that this tradition continues. Parents are welcome to take photographs of their own children at award ceremonies, setting concerts/shows and sporting events, with the permission of the Headteacher/Senior Manager or Childminder. However, care must be taken not to interfere with the smooth running of the event, breach commercial copyright laws or compromise health and safety. Parents/carers will ensure that:

- They will respect the setting's decision to prohibit photography of certain children or a particular event.
- Any images taken are for personal use only.

---

<sup>1</sup> The LA recommends on admission to a setting with at least annual updates

- Images including children **other than their own, must not be sold or put on the internet**; if they are, Data Protection legislation may be contravened and they will be asked to remove them.
- They will not use any images of children so as to cause offence or harm.

## **The Use of Cameras and Video Recordings by Children**

From time to time, children may be given the opportunity to use setting equipment to take photographs and/or video footage as part of a curricular or extra-curricular activity.

Children should not use personal equipment in the setting for the purpose of taking photographs or video footage, unless being used as a learning resource in line with the setting's Acceptable Use policy. This includes the use of personal Smartphones. The only exception to this is on a setting trip or visit where children may be allowed to take photographs for their own personal use.

It should be made clear that these images should be taken responsibly and not used to upset any other child

**The use of images to bully or intimidate, including publishing photographs without permission on the internet, will be dealt with in line with the setting's behaviour and anti-bullying policies and may be viewed as a criminal offence.**

## **Display of photographs**

It is perfectly acceptable to display photographs of children in the setting environment with their names attached for the purpose of celebrating progress and achievement or assessment purposes.

However, all settings must give consideration to displays when rooms are available for other purposes.

## **Publicity**

### **Press**

On occasions, the media are asked to cover setting events or to highlight children's successes. This is an important part of celebrating achievement and informing the public of educational initiatives. The media operate under their own Code of Practice. Parents will be informed by the setting in advance if their children are likely to appear in the press. Local newspaper titles may share their images with other titles within the same syndicate. Any child whose parents have withheld permission, will not be photographed by the media.

### **Setting Publicity**

Photographs of children's activities and achievements may be published in the setting newsletter or prospectus and posted on the setting website. Names of individual children will not be attached to photographs and no contact details will be published. Where photographic permission has been withheld, photographs will not be published.

### **Setting Photographer**

Class and individual or group photographs are often an annual event. Parents will be notified in advance of the photographer's visit and will be sent copies of photographs and given the option to purchase them. Copyright on all such photographs is retained by the photographer.

## **Links**

This guidance should link specifically to the setting's Data Security Policy, Online safety Policy, Acceptable Use Policy, Password Policy, Staff Laptop Policy, Safeguarding Children Policy and to the LA guidance 'Schools System and Data Security'.

### **Further Guidance**

Further related guidance can be found in the Becta series of documents entitled *Good practice in information handling in schools*. They are:

- 1 Keeping data secure, safe and legal
- 2 Impact levels and labelling
- 3 Audit logging and incident handling
- 4 Data encryption
- 5 Secure remote access

and also in *AUPs in context: Establishing safe and responsible online behaviours*

These documents can be found on Edulink ([www.edulink.networcs.net](http://www.edulink.networcs.net)) and on the Department for Education website ([www.education.gov.uk](http://www.education.gov.uk)).



### 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? *(Please note that the use of photographs in newspapers is subject to strict guidelines)* Yes / No
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

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 **their child/ children** at events such as, 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. **The Headteacher / Senior Manager will explain when images/recordings may be taken at such events.** 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 parent / carer: .....

Signed: ..... Date: .....

**Data Protection** Tenacres 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.

## Appendix 8 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), parents or carers as 'friends'.
- 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](mailto: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.***

<b>Name</b>		<b>Date</b>	
-------------	--	-------------	--

## Appendix 9 Loaned Device User Agreement

The Headteacher has agreed that a laptop computer will be loaned to you while you remain employed at this school. This loan is subject to review on a regular basis and can be withdrawn at any time.

As a member of staff to whom a laptop has been loaned, I have read and agree to the following terms and conditions that apply while the laptop is in my possession:

- The Laptop and any accessories provided with it, remains the property of Tenacres First School and is strictly for my sole use in assisting in the delivery of the Curriculum. It is not for personal use, e.g. Facebook or other social networking sites or on-line shopping.
- I understand insurance cover provides protection from the standard risks but excludes theft from a vehicle.
- If left unattended the laptop must be securely stored. It must **never** be left unattended even for a short period in a car, including in a locked boot.

- I agree to treat the laptop with due care and keep the laptop in good condition. I will ensure that it is strapped in to the carry case when transported and/or not in use, not leave the laptop unattended in class and avoid food and drink near the keyboard/touch pad.
- I agree to backing up my work on a regular basis. I understand the school will not accept responsibility for the loss of work in the event of the laptop malfunctioning.
- I agree to only use software licensed by the school, authorised by Jon Beacham or our Peritech team.
- I agree that Anti-Virus software is installed and must be updated on a weekly basis. Our Peritech team will advise on the routines and schedule of this operation.
- Should any faults occur, I agree to notify Jon Beacham or the Peritech team as soon as possible so that they may undertake any necessary repairs. Under no circumstances should I, or anyone other than ICT staff, attempt to fix suspected hardware faults.
- I agree to attend training in how to access the Curriculum Network, Intranet, VLE , Internet, and email within the school provided by Jon Beacham, our Peritech team or any outside provides.
- I agree that home Internet access is permitted at the discretion of the Headteacher. I understand the school will not accept responsibility for offering technical support relating to home Internet connectivity.
- I agree that any telephone/broadband charges incurred by staff accessing the Internet from any site other than school premises are not chargeable to the school.
- I agree to adhere to School and LA policies regarding the following, updated as necessary:
  - Acceptable Use;
  - Data Protection;
  - Computer Misuse;
  - Health and Safety.
- I agree to use a secure password including numbers, uppercase letters and/ or special characters.

**Laptop Details**

Make	Model	Serial Number

**Personnel Details**

Loan Authorised by .....

Headteacher: ..... (signature) Date .....

**I have read and agree to be bound by the terms and conditions set out above.**

I agree that my laptop is brought into school **on a Thursday** for regular maintenance.

Name of Member of Staff ..... (Print)

Received by (signature): ..... Date .....