# Astley C.E. Primary School Online Safety Policy

## Our Vision and Values


Ratified by the Governing Body: October 2021

Date for review: October 2023

Signed by: Chair of governors : Marc Stevenson

Headteacher : Tracie Langfield

## Contents

## 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 addITive 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.

## SECTION A – Policies

## 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 IT. It also outlines the core responsibilities of all users of IT 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 IT

### A.1.1 Responsibilities: the e-safety committee

Astley School has an e-safety committee led by our e-safety co-ordinator and is made up of the e-safety co-ordinator, head teacher and e-safety governor. This committee is responsible for:

- Review and monitoring of this e-safety policy.
- Consider any issues relating to school filtering (see section B.2.1 of this policy)
- Discuss any e-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 bodies outside the school such as the Worcester Safeguarding Children Board (WCF).

### A.1.2 Responsibilities: e-safety coordinator

E-safety lead – Mrs Tracie Langfield.

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

- Leads the e-safety committee
- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident
- Provides training and advice for staff
- Liaises with the Local Authority
- Liaises with school IT technical staff
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- Reviews weekly the output from monitoring software and initiates action where necessary
- Meets regularly (termly) with e-safety governor to discuss current issues, review incident logs and filtering change control logs
- Attends relevant meetings and committees of Governing Body
- Reports regularly to headteacher
- Receives appropriate training and support to fulfil their role effectively
- Provides information to parents on key initiatives in school.

## A.1.3 Responsibilities: governors

Astley School governors are responsible for the approval of this policy and for reviewing its effectiveness. This will be carried out by the governors (delegated to the Resources Committee) receiving regular information about e-safety incidents and monitoring reports. A member of the governing body has taken on the role of e-safety governor which involves:

- Regular meetings with the e-safety leader (termly) with an agenda based on:
- Monitoring of e-safety incident logs
- Monitoring of filtering change control logs
- Reporting to relevant governors committee/meeting

## A.1.4 Responsibilities: head teacher

The head teacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety is delegated to the e-safety leader.

- The head teacher will be familiar with the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff, including non-teaching staff. (see flow chart on dealing with e-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 e-safety matters and of the current 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 schools' Acceptable Use policy for staff (see Appendix 1)
- They report any suspected misuse of problem to the e-safety coordinator
- Digital communications with students (email/learning platform/voice) should be on a professional level and only carried out using official school systems (please see A.3.5)
- E-safety issues are regularly taught and embedded in the curriculum, and other school activities (please see section C)
- They appropriately supervise the use of technology by children in their care. (Children should not be allowed to search You Tube, for example.)

## A.1.6 Responsibilities: IT technician

The IT technician is responsible for ensuring that:

- The school's IT infrastructure is secure and is not open to misuse or malicious attack
- The school meets the e-safety technical requirements outlined in section B.2.2 of this policy (and any relevant Local Authority e-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 IT coordinator or head teacher so that appropriate action may be taken.

## A.2.1 Policy development, monitoring and review

This e-safety policy has been developed by a working group made up of:

- School e-safety coordinator
- Head teacher
- Teachers
- Support staff
- IT technical staff
- Governors

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

- Staff meetings
- Governor Curriculum Committee meetings

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

| | |
|---|---|
| **This e-safety policy was approved by the governing body on:** | |
| **The implementation of this e-safety policy will be monitored by the:** | *Mrs Tracie Langfield (E-safety co-ordinator)* |
| **Monitoring of this policy will take place at regular intervals:** | *Termly* |
| **The governing body will receive regular reports on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) as part of a standing agenda item with reference to safeguarding:** | Termly (the e-safety coordinator sits on the governing body) |
| **The e-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 e-safety or incidents that have taken place. The next anticipated review date will be:** | *Annually monitored - October 2023* |
| **Should serious e-safety incidents take place, the following external persons / agencies should be informed:** | *Worcestershire Safeguarding Children Partnership (WCF)*<br><br>*Local Authority Designated Officer*<br><br>*Worcestershire Senior Adviser for Safeguarding Children in Education – Denise Hannibal*<br><br>*West Mercia Police* |

## A.2.2 Policy Scope

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

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

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

## A.2.3 Acceptable Use policies

All members of the school community are responsible for using the school IT systems in accordance with the appropriate acceptable use policy, 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 (KS1 & KS2)
- Staff and volunteers
- Parents/carers
- Technical support personnel

Acceptable Use Agreements are introduced at parents' induction meetings and signed by all pupils as they enter Astley School (with parents signing on behalf of children below Year 3).

Prior to Year 3, the AUA is discussed verbally with children on a regular basis so that children are aware of the importance of its contents. Acceptable Use Agreements are signed by all children as they enter Key Stage 2.

Staff and volunteers sign when they take up their role in school and in the future if significant changes are made to this 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 schools IT resources (including the internet) and permission to publish their work.

## A.2.4 Self evaluation

Evaluation of e-safety is an on-going process and links to other self-evaluation tools used in school in particular to pre Ofsted evaluations along the lines of the School Evaluation Form (SEF). The views and opinions of all stakeholders (pupil, parent and 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 IT policies:*

- **IT policy** – how IT is used, managed, resourced and supported in our school.
- **Computing curriculum** - key documents and associated resources directly relating to learning covering the Computing Curriculum

*Other policies relating to e-safety*

- **Anti-bullying** – how our school strives to illuminate bullying – links to cyber bullying.
- **RSE/PSHE** – e-safety has links to this – staying safe.
- **Safeguarding** – safeguarding children electronically is an important aspect of e-safety. The e-safety policy forms a part of the school's safeguarding policy.
- **Behaviour** – linking to positive strategies for encouraging e-safety and sanctions for disregarding it.
- **Use of images** - WCF guidance to support the safe and appropriate use of images in schools, academies and settings

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

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

- Users shall not visit internet sites, make, post download, upload, data transfer, communicate or pass on, material, remarks, proposal or comments that contain or relate to:
- **Child sexual abuse images (illegal – The Protection of Children Act 1978)**
- **Grooming incitement, arrangement or facilitation of sexual acts against children (illegal – Sexual Offences Act 2003)**
- **Possession of extreme pornographic images (illegal – Criminal Justice and Immigration Act 2008)**
- **Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) (illegal – Public Order Act 1986)**
- Pornography
- Promotion of any kind of discrimination
- Promotion of racial or religious hatred
- Threatening behaviour, including promotion of physical violence or mental harm,
- Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or bringing the school into disrepute.

Additionally the following activities are also considered unacceptable on IT kit provided by the school:

- Using school systems to undertake transactions pertaining to a private business
- Use systems, application, website or other mechanisms that bypass the filtering or other safeguards employed by the school and Worcestershire County Council.
- Uploading, downloading or transmitting commercial software or any other copyrighted materials belonging to third parties, without the necessary licensing permissions
- Revealing or publicising confidential or propriety 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
- Use of social networking sites (other than 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 follows:

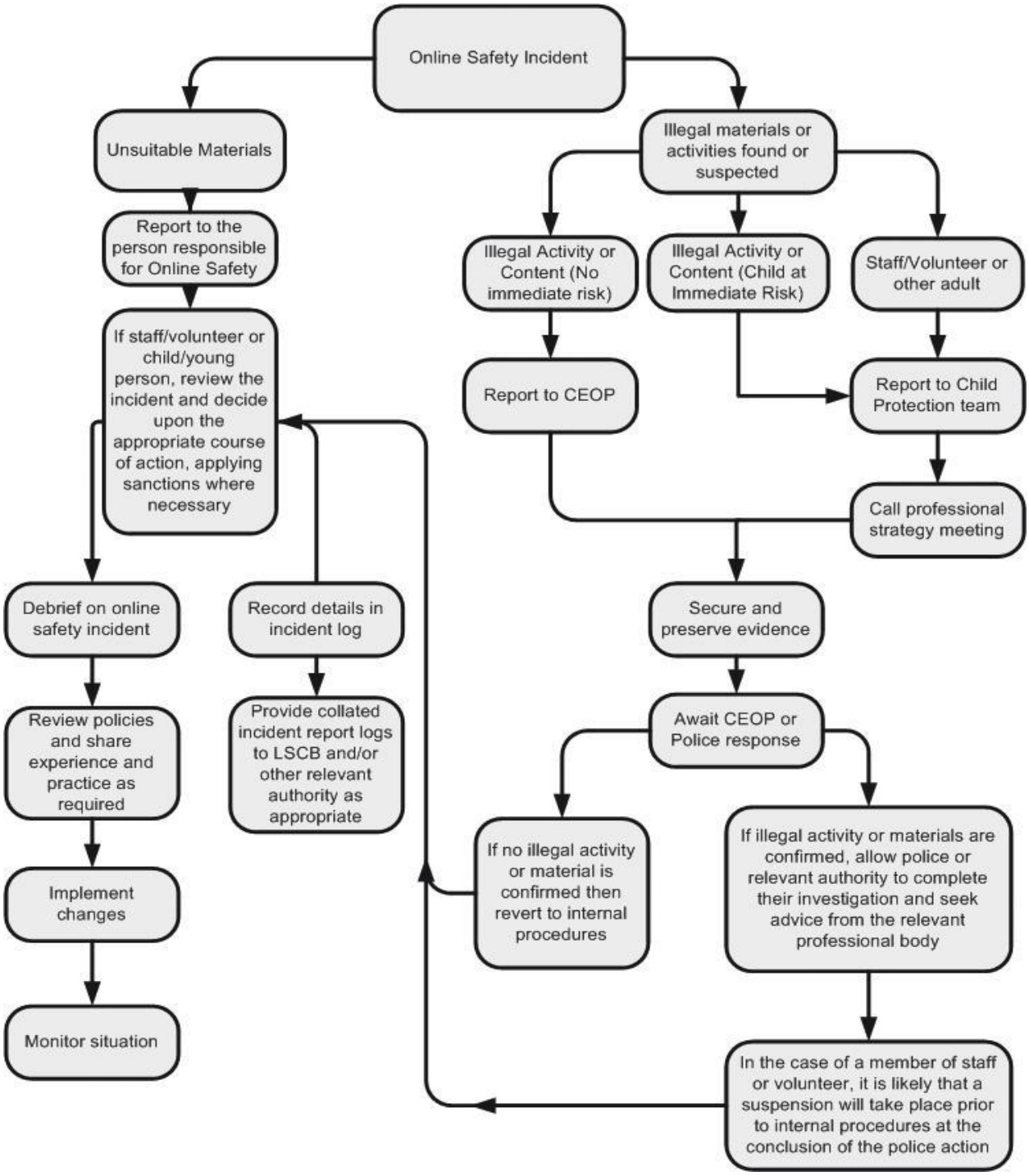
| **Pupil sanctions** | Refer to class teacher | Refer to e-safety coordinator | Refer to head teacher | Refer to police | Take action on filtering | Inform parents/carers | Removal of access | Warning |
|---|---|---|---|---|---|---|---|---|
| Deliberately accessing or trying to access material that could be considered illegal. | | ✓ | ✓ | | ✓ | ✓ | | ✓ |
| Unauthorised use of non-education 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, 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 materials and failing to report the incident. | ✓ | ✓ | ✓ | | ✓ | ✓ | | |

| Staff sanctions | Refer to head teacher | Refer to local authority/HR | Refer to police | Seek filtering advice | Warning | Suspension | Disciplinary action |
|---|---|---|---|---|---|---|---|
| Deliberately accessing or trying to access material that could be considered illegal. | ✓ | ✓ | | ✓ | ✓ | | ✓ |
| Excessive or inappropriate personal use of the internet/personal email. | ✓ | ✓ | | | | | |
| Unauthorised downloading or uploading of files. | ✓ | | | ✓ | | | |
| Allowing others to access school network by sharing usernames 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 carry out digital communications with pupils. | ✓ | ✓ | | ✓ | | | |
| Actions which could compromise the staff member's professional standing. | ✓ | ✓ | | | | | |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school. | ✓ | ✓ | | | | | |
| Using proxy sites or other means to subvert the school's filtering system. | ✓ | | | ✓ | | | |
| Accidentally accessing offensive or pornographic materials and failing to report the incident. | ✓ | | | ✓ | | | |
| Deliberately accessing or trying to access offensive or pornographic material. | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ |
| Breaching copyright or licensing regulations. | ✓ | | | | | | |
| Continued infringements of the above, following previous warnings or sanctions. | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ |

## A.2.7 Reporting of e-safety breaches

It is hoped that all members of Astley School community will be responsible users of IT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless, 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 hand held devices)

Astley School recognises 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 as follows:

- 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.
- 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 of pupil contact 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.

| **Personal hand held technology** | Staff/adults | | | Pupils | | | |
|---|---|---|---|---|---|---|---|
| | Allowed | Allowed at certain times | Not allowed | Allowed | Allowed at certain times | Allowed with staff | Not allowed |
| Mobile phones may be brought to school | ✓ | | | | | | ✓ |
| Use of mobile phones in lessons | | ✓ | | | | | ✓ |
| Use of mobile phones in social time | | ✓ | | | | | ✓ |
| Taking photos on personal phones/devices | | | ✓ | | | | ✓ |
| Use of hand held devices e.g. PDAs, gaming consoles | | | ✓ | | | | ✓ |

## A.3.2 Use of communication technologies

### A.3.2a – Email

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

- These official school email services may be regarded as safe and secure and are monitored.
- Staff should only use the school email services to communicate with others when in school or on school systems (by remote access)
- Users need to be aware that email communications may be monitored

- Users must immediately report to their teacher / e-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 times | Not allowed | Allowed | Allowed at certain | 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 | Not allowed | Allowed | Allowed at certain | 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. 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 education aims, but must follow school policies concerning the sharing, distribution and publication of those images.
- Those **images should only be captured using school equipment; the personal equipment of staff should not be used for such purposes.**

- The school gains consent for all children's images to be used (without names accompanying) on the school website when pupils start school.
- When staff seek to publish children's images they should first check the list of children not permitted to be used, which is kept in the school office.
- 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 Use of web-based publication tools

Astley School uses the public facing website (www.astley.worcs.sch.uk) for sharing information with the community beyond our school. This includes, from time-to-time celebrating work and achievements of children. All users are required to consider good practice when publishing 'public' content.

- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.
- Only pupil's first names are 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 meet with the following good practice guidance on the use of such images:
- Pupil's full names will not be used anywhere on a website or blog, and never in association with photographs
- Images that can easily be reedited are not posted in public areas
- 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)

## A.3.5 Professional standards for staff communication

In all aspects of their work in our school, teachers abide by the broad Professional standards for teachers laid down by the TDA and the Teacher's standards as describe by the DfE (effective 2012). Teachers translate these standards appropriately for all matters relating to e-safety.

- Any digital communication between staff and pupils or parents/carers (email) 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 evaluation help inform policy and develop practice.

# Section B. Infrastructure

## B.1 Password security

Teachers frequently discuss issues relating to password security and how it relates to staying safe in and out of school.

## B.2.1 Filtering

## B.2.1a – Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot however, provide a 100% guarantee that it will do so. It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in school.

As a school buying Broadband services from Worcestershire County Council, Astley School automatically receive the benefits of a managed filtering service with some flexibility for changes at local level.

The school also uses the Futures Digital monitoring software to enhance the safety and security of our school system. This software generates weekly report logs that are sent to the Office Manager and reviewed by the e-safety lead.

## B.2.1b Responsibilities

The day-to-day responsibility for the management of the school's filtering policy is held by the e-safety coordinator (with ultimate responsibility resting with the head teacher and governors). They manage the school 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 school filtering service must:

- Be logged in to change control logs
- Be reported to a second responsible person (the head teacher/e-safety governor) within the time frame stated in section A.1.3 of this policy.
- Be reported to, and authorised by, a second responsible person prior to changes being made (this will normally be the class teacher who originally made the request for the change)

All users have a responsibility to report immediately to class teachers/e-safety coordinator any infringements of the school's 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 e-safety education programme. (See section C of this policy)

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

- Signing the AUA (a part of their induction process)
- Briefing in staff meetings, training days, memos etc... (from time to time and on-going)

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement and through e-safety awareness sessions/newsletter.

## B.2.1d – Changes to the filtering system

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

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

The e-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.

## B.2.1e – Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. Astley school staff will ensure the monitoring of users activities on the school network and on the school equipment using the Future Digital software to support this work.

- The e-safety co-ordinator reviews 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 e-safety governor within the timeframe stated in section A.1.3 of this policy
- the e-safety committee (see A.1.1)
- the Worcestershire Safeguarding Children Partnership 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 by Chestnut Infrastructure. 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 Chestnut Infrastructure. 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 Astley School (see section C of this policy)

# Section C Education

## C.1.1 E-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 e-safety is therefore an essential part of Astley School's e-safety provision. Children and young people need constant help and support to recognise and avoid e-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.

E-Safety education will be provided in the following ways:

- A planned e-safety programme is provided as part of IT, RSE/PSHE and other lessons and will be regularly revisited – this will cover both the use of IT and new technologies in school and outside school.
- Key e-safety messages will be reinforced through further input via assemblies and pastoral activities as well as informal conversations when the opportunity arises.
- Pupils will be helped to understand the need for the pupil AUA and encouraged to adopt safe and responsible use of IT both within and outside school.
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- When pupils are allowed to freely search the internet e.g. using search engines, staff should be vigilant in monitoring the content of the websites that pupils 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 technologies 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

- Pupils should 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 e-safety education http://www.thinkuknow.co.uk/teachers/resources/. These are mediated by a CEOP trained teacher.

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

At Astley School it is our policy to ensure that our children play a leading role in shaping the way our school operates and this is very much the case with our e-learning strategy. Our children often use technology out of school in ways that we do not in school and members of staff are always keen to hear of children's experiences and how they feel the new technology, especially rapidly developing technology (such as mobile devices) could be helpful in their learning.

## C.2 Staff training

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

- A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and acceptable use polices which are signed as part of their induction.
- The E-safety Co-ordinator (or another member of staff such as the Safeguarding Officer) will be CEOP trained.
- The E-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 WSCP and others.
  All teaching staff have been involved in the creation of this e-safety policy and are therefore aware of its content.
- The E-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 e-safety training/awareness sessions, with particular importance for though who are members of the Curriculum Committee or group involved in IT, e-safety, health and safety or child protection. This may be offered in a number of ways:

- Participation in school training/information sessions for staff or parents
- Attendance at training provided by the Local Authority

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

## C.4 Parent/carer awareness raising

Some parents/carers have only a limited understanding of e-safety risks 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 underestimate or do not realise how often children 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).

Astley School will provide information and promote awareness to parents and carers through:

- Letters, newsletters, website
- Parent’s evenings and information events
- Reference to the parents materials on the Think U know website (http://www.thinkuknow.co.uk)

## C.5 Wider community understanding

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

## Acceptable Use Agreement for all pupils in Reception and KS1

## This is how we stay safe when we use computers:

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

I have discussed these rules with my child to help them understand how to stay safe when using computers, laptops and ipads in school.

My child will do his/her best to keep them.

| | |
|---|---|
| Parents name: | |
| Signed (parents): | |
| Child's name: | |
| Signed (child): | |

## Acceptable Use Agreement for all pupils in KS2

I understand that while I am a member of Astley School I must use technology in a responsible way.

### For my own personal safety:

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

### For the safety of others:

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

### For the safety of the school:

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

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

| | |
|---|---|
| Name: | |
| Signed: | |
| Date: | |

## Acceptable Use Agreement for all staff & volunteers

### 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 IT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the IT systems and other users. I will, where possible, educate the young people in my care in the safe use of IT and embed e-safety in my work with young people.

### For my professional and personal safety:

- I understand that the school will monitor my use of the IT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school IT systems (e.g. laptops, email, learning platform) out of the school.
- I understand that the school IT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down in the e-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 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.
- 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 e-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 IT devices as agreed in the e-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 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 or Entrust**).

- 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/academy:**

- I understand that this Acceptable Use Agreement applies not only to my work and use of school IT equipment in the school, but also applies to my use of school IT 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/academy IT systems (both in and out of the school) within these guidelines.**

| | |
|---|---|
| Staff / volunteer Name: | |
| Signed: | |
| Date: | |

## Acceptable Use Agreement and permission forms – parent / carer

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

This Acceptable Use Agreement is intended to ensure that:

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

Astley School will try to ensure that pupils will have good access to IT to enhance their learning and will, in return, expect them to agree to be responsible users.

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

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

## Permission for my child to use the internet and electronic communication

As the parent / carer of the above pupil(s), I give permission for my son / daughter to have access to the internet and to IT systems at Astley School.

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe and responsible use of IT – both in and out of Astley School.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and IT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the IT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Agreement.

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

| | |
|---|---|
| Parent's signature: | |
| Date: | |

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

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

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

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

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

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

| | |
|---|---|
| Parent's signature: | |
| Date: | |

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

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

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

| | |
|---|---|
| Parent's signature: | |
| Date: | |

## Appendix 2 - Guidance for Reviewing Internet Sites

This guidance is intended for use when Astley 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 Future Digital from Forensic 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 e-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/e-safety/ **WMNet** – http:// www.wmnet.org.uk

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

### Cyber Bullying

**Teachernet "Safe to Learn – embedding anti-bullying work in schools"** (Archived resources) http://tna.europarchive.org/20080108001302/http://www.teachernet.gov.uk/wholeschool/academy/behaviour/tacklingbullying/cyberbullying/

**Anti-Bullying Network** -

http://www.antibullying.net/cyberbullying1.htm **Cyberbullying.org** -

http://www.cyberbullying.org/

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

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

### Social networking

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

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

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

## Mobile technologies

**"How mobile phones help learning in secondary schools":**

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

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

## Data protection and information handling

**Information Commissioners Office** - Data Protection:

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

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

http://www.digitalparenting.ie/

https://www.commonsensemedia.org/

## Links to other resource providers

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

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

Kidsmart:

http://www.kidsmart.org.uk/default.aspx Know It

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

Cybersmart -

http://www.cybersmartcurriculum.org/home/ Internet

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

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

## Appendix 5 - Glossary of terms

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

## Appendix 6 Template Reporting Log

**Reporting Log**

Group ……

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

## 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 pITure. Including brief information and an unidentifiable pITure, 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 frITion in your school and make your working environment uncomfortable.

- Do not post or upload photographs related to school-based or extra-curricular activities and do not make specific reference to your school in any post as comments may be misconstrued and result in inappropriate responses.

- Be aware of any spam or potential virus risks sent via rogue posts. It is advisable to check with anti-virus firms if you get any suspicious requests or posts.

- If you are alerted to any negative or unscrupulous information about yourself, colleagues or your school on Facebook or other social networking sites, inform your headteacher. Further advice to help with cyberbullying incidents etc., can be gained from help@saferinternet.org.uk (0844 3814772) or a professional association such as your Trade Union.

- ***I understand the implications of using Facebook and other social networking sites for my own protection and professional reputation, as well as the impact that my use can have on my school community and establishment.***
- ***I understand that injudicious use of social networking may lead to disciplinary action.***
- ***I agree to take all possible precautions as outlined above.***

| ***Name*** | | ***Date*** | |
|---|---|---|---|

# Appendix 9 Loaned Device User Agreement

Staff member: Date:

Device Make: Model : Serial Number :
The laptop/device detailed above is loaned to Xxxxxxxxxxx Xxxxxxxxxx for the duration of their employment at Xxxxxxxxxxxxxx Xxxxxxx School subject to the following terms and the school Acceptable Use Agreement.

The iPad/mobile device remains the property of the School and must be returned at the end of the contracted period of employment with the School and, if required, during a planned or prolonged absence.

1. The laptop/device is for the **work related** use of the named member of staff to which it is issued.

2. Only software/apps installed at the time of issue or software/apps purchased by and licensed to Xxxxxxxxxxxxx Xxxxxxx School may be installed on the machine.

3. The laptop/device remains the property of the School throughout the loan period, however the member of staff to which it is issued **will** be required to take responsibility for its care and safe keeping.

4. If left unattended the laptop/device must be securely stored. It must **never** be left unattended even for a short period in a car, including in a locked boot.

5. Due regard must be given to the security of the computer if using other forms of transport.

6. In order to ensure the schools compliance with the Data Protection Act and to avoid breaches of confidentiality, under no circumstances should students be allowed to use the staff laptops/devices if not directly supervised by a member of staff. Staff should also be cautious when using the computer away from school particularly with files which may contain personal student data, including images.

7. The equipment must be docked in the school charging and syncing cabinet at least once per week to ensure updates and new software are distributed. Staff should record this action in the log provided with the syncing cabinet.

8. The laptop/device will be recalled from time to time for routine maintenance / upgrade and monitoring.

**Prohibited Uses**

Images of other people, including children, may only be made with the permission of the person, or parents of the child, in the photograph.

The laptop/device is a professional tool designed to enhance classroom practice. It is not for personal use, e.g. Facebook or other social networking sites or on-line shopping, and should remain in school unless permission is sought from the IT Co-ordinator or Head Teacher.

**Lost, Damaged or Stolen laptop/device**

If the laptop/device is lost, stolen or damaged, the IT Co-ordinator or Head Teacher must be informed immediately and a charge may be levied depending on the circumstances.

I have read and agree to the terms and conditions in this agreement.
I undertake to take due care of the laptop or device and return it immediately upon request.

Signed: _____

Date: _____