

DODFORD FIRST SCHOOL



E-SAFETY POLICY

Contents

| | |
|---|-------|
| Contents | 2 |
| Background and rationale..... | 4 |
| Section A - Policy and leadership..... | 5 |
| A.1.1 Responsibilities: the e-safety committee..... | 5 |
| A.1.2 Responsibilities: e-safety coordinator..... | 5 |
| A.1.3 Responsibilities: governors | 5 |
| A.1.4 Responsibilities: head teacher..... | 6 |
| A.1.5 Responsibilities: classroom based staff | 6 |
| A.1.6 Responsibilities: ICT technician | 6 |
| A.2.1 Policy development, monitoring and review | 7 |
| Schedule for development / monitoring / review of this policy..... | 8 |
| A.2.2 Policy Scope..... | 8 |
| A.2.3 Acceptable Use Agreements | 9 |
| A.2.4 Self Evaluation | 9 |
| A.2.5 Whole School approach and links to other policies..... | 9 |
| Core ICT policies | 9 |
| Other policies relating to e-safety | 10 |
| A.2.6 Illegal or inappropriate activities and related sanctions | 10-14 |
| A.3.1 Use of hand held technology (personal phones and other hand held devices) | 15 |
| A.3.2 Use of communication technologies..... | 17 |
| A.3.2a - Email..... | 17 |
| A.3.2b - Social networking (including chat, instant messaging, blogging etc) | 18 |
| A.3.2c - Videoconferencing..... | 18 |
| A.3.3 Use of digital and video images | 18 |
| A.3.4 Use of web-based publication tools..... | 19 |
| A.3.4a - 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 | 20 |
| B.1 Password security | 20 |
| B.2.1 Filtering..... | 21 |
| B.2.2 Technical security..... | 22 |
| B.2.3 Personal data security (and transfer) | 22 |

| | |
|--|----|
| Section C. Education..... | 23 |
| C.1.1 E-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..... | 25 |
| C.5 Wider community understanding..... | 25 |

Appendix 1:

| | |
|--|----------|
| A - Acceptable User Agreement Foundation..... | 26 |
| B - Acceptable User Agreement Key Stage One | 27 |
| C - Acceptable User Agreement Key Stage Two | 28 |
| D - Acceptable User Agreement Staff | 29,30,31 |
| E - Acceptable User Agreement Parents and Carers | 32-34 |
| F - Acceptable User Agreement Community User | 35-36 |
| G - Acceptable User Agreement Governor | 37 |

Appendix 2:

| | |
|-----------------------------------|-------|
| Guidance Reviewing Websites | 38-39 |
|-----------------------------------|-------|

Appendix 3:

| | |
|-------------------------------------|----|
| Criteria for website filtering..... | 40 |
|-------------------------------------|----|

Appendix 4:

Supporting resources and links

Appendix 5:

| | |
|------------------------|-------|
| Glossary of terms..... | 43-44 |
|------------------------|-------|

Appendix 6:

| | |
|----------------------------------|----|
| Template for reporting log | 45 |
|----------------------------------|----|

Background and rationale

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

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

- Access to illegal, harmful or inappropriate images or other content
- Allowing or seeking unauthorised access to personal information
- Allowing or seeking unauthorised access to private data, including financial data
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive or addictive use which may impact on social and emotional development and learning.
- The potential to be drawn into terrorism through radicalisation via social media

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

Our 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 E-Safety Policy and keeping everyone safe with ICT. It also outlines the core responsibilities of **all users** of ICT in our school/academy.

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

A.1.1 Responsibilities: the e-safety committee

The school council regularly discusses issues relating to e-safety. Issues that arise are referred to other school bodies as appropriate and when necessary to bodies outside the school such as the Worcestershire Safeguarding Children Board.

A.1.2 Responsibilities: e-safety coordinator

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 any e-safety discussions.
- 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 ICT 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 with e-safety governor to discuss current issues and review incident logs
- attends relevant meetings and committees of Governing Body
- reports regularly to the Headteacher
- 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 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 Co-ordinator with an agenda based on:*
 - *monitoring of e-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 e-safety) of all members of the school community, though the day to day responsibility for e-safety is delegated to the E-Safety Co-ordinator.
- 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 school/academy e-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.
- they report any suspected misuse or problem to the E-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 e-safety issues in the curriculum and other activities, also acknowledging the planned e-safety programme (see section C)

A.1.6 Responsibilities: ICT technician

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/academy 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/academy's e-security policy
- shortcomings in the infrastructure are reported to the ICT coordinator or head teacher so that appropriate action may be taken.

A.2.1 Policy development, monitoring and review

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

- *School E-Safety Coordinator*
- *Safeguarding officer*
- *Head teacher*
- *Teachers*
- *Support staff*
- *Governors (especially the e-safety governor)*
- *Pupils*

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

- *Staff meetings*
- *School Council*
- *Governor's meeting / subcommittee meeting*
- *School website/ newsletters*

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: | <i>Headteacher</i> |
| Monitoring of this policy will take place at regular intervals: | <i>Annually</i> |
| 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: | <i>Annually</i> |
| 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: | <i>Each Summer term</i> |
| Should serious e-safety incidents take place, the following external persons / agencies should be informed: | <i>Worcestershire Safeguarding Children Board Local Authority Designated Officer Worcestershire Senior Adviser for Safeguarding Children in Education West Mercia Police</i> |

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/academy ICT systems, **both in and out of school**.

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 e-safety incidents covered by this policy, which may take place out of the school/academy, 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 e-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/academy ICT systems in accordance with the appropriate Acceptable Use Agreement (AUA), which they will be expected to sign before being given access to school/academy systems.

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

- Pupils
- Staff (and volunteers)
- Parents / carers
- Governing Body
- Community users of the school's ICT system

Acceptable Use Agreements are introduced at parents' induction meetings and are signed by parents on behalf of their children in reception and by children in Years 1 and 2.

Pupils re-sign on entering Key Stage 2.

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

A.2.5 Whole School approach and links to other policies

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

Core ICT policies

| | |
|------------------------|---|
| ICT Policy | How ICT is used, managed, resourced and supported in our school. |
| E-Safety Policy | How we strive to ensure that all individuals in school stay safe while using Learning Technologies. The e-safety policy constitutes a part of the ICT policy. |

| | |
|--|---|
| School systems and Data Security Policy | How we categorise, store and transfer sensitive and personal data and protect systems. This links strongly and overlaps with the e-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 e-safety

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

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 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/academy community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as indicated on the following pages:

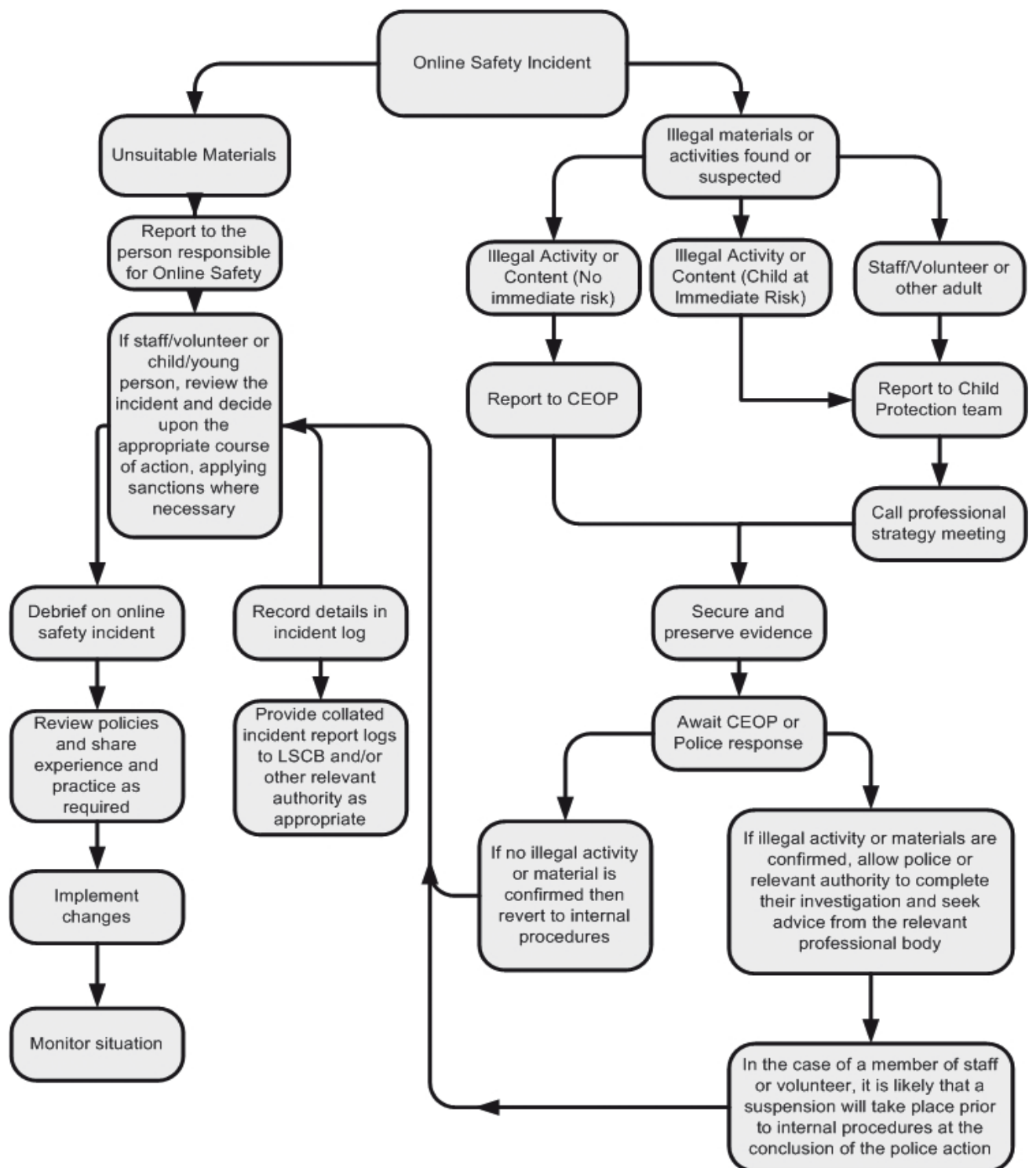
| | Refer to: | | | | | Inform: | Action: | | |
|--|---------------|----------------------|-----------------------|-----------------|--|------------------|--|---------|---|
| | Class teacher | E-safety coordinator | Refer to head teacher | Refer to Police | Refer to e-safety coordinator for action re filtering / security etc | Parents / carers | Remove of network / internet access rights | Warning | Further sanction e.g. detention / exclusion |
| Pupil sanctions <i>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.</i> | | | | | | | | | |
| Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities). | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Unauthorised use of non-educational sites during lessons | ✓ | | | | ✓ | | | | |
| Unauthorised use of mobile phone / digital camera / other handheld device | ✓ | | | | | ✓ | ✓ | | |
| Unauthorised use of social networking / instant messaging / personal email | ✓ | ✓ | | | ✓ | ✓ | | ✓ | |
| Unauthorised downloading or uploading of files | ✓ | | | | | | ✓ | ✓ | |
| Allowing others to access school/academy network by sharing username and passwords | ✓ | ✓ | ✓ | | ✓ | | ✓ | ✓ | |
| Attempting to access the school/academy network, using another pupil's account | ✓ | | | | ✓ | | ✓ | | |
| Attempting to access or accessing the school/academy network, using the account of a member of staff | ✓ | | ✓ | | ✓ | ✓ | | ✓ | |
| Corrupting or destroying the data of other users | ✓ | | ✓ | | ✓ | ✓ | ✓ | ✓ | |
| Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | |
| Continued infringements of the above, following previous warnings or sanctions | ✓ | ✓ | ✓ | | | ✓ | ✓ | | ✓ |
| Actions which could bring the school/academy into disrepute or breach the integrity of the ethos of the school/academy | ✓ | | ✓ | | | | | ✓ | |
| Using proxy sites or other means to subvert the school/academy's filtering system | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | |
| Accidentally accessing offensive or pornographic material and failing to report the incident | ✓ | ✓ | | | ✓ | ✓ | | | |
| Deliberately accessing or trying to access offensive or pornographic material | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | | ✓ |
| Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act | ✓ | | ✓ | | ✓ | | ✓ | | |

| | Refer to: | | | | | Action: | | |
|--|--------------|--------------|----------------------|--------|---|---------|------------|---------------------|
| | Line manager | Head teacher | Local Authority / HR | Police | Technical Support Staff for action re filtering etc | Warning | Suspension | Disciplinary action |
| Staff sanctions | | | | | | | | |
| <i>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.</i> | | | | | | | | |
| Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities). | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ |
| Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email | ✓ | ✓ | | | | ✓ | | |
| Unauthorised downloading or uploading of files | ✓ | | | | ✓ | ✓ | | |
| Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school/academy network, using another person's account | ✓ | ✓ | | | ✓ | ✓ | ✓ | |
| Careless use of personal data e.g. holding or transferring data in an insecure manner | ✓ | ✓ | ✓ | | ✓ | ✓ | | ✓ |
| Deliberate actions to breach data protection or network security rules | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | |
| Corrupting or destroying the data of other users or causing deliberate damage to hardware or software | | ✓ | ✓ | | | | ✓ | ✓ |
| Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature | ✓ | ✓ | | | | ✓ | ✓ | |
| Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils | ✓ | ✓ | | | ✓ | | | |
| Actions which could compromise the staff member's professional standing | ✓ | ✓ | | | | | | |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school | ✓ | | | | | ✓ | | |
| Using proxy sites or other means to subvert the school's filtering system | ✓ | | | | ✓ | ✓ | | ✓ |
| Accidentally accessing offensive or pornographic material and failing to report the incident | ✓ | ✓ | | | ✓ | ✓ | | |
| Deliberately accessing or trying to access offensive or pornographic material | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ |
| Breaching copyright or licensing regulations | ✓ | | | | | ✓ | | |
| Continued infringements of the above, following previous warnings or sanctions | ✓ | ✓ | | | ✓ | | | ✓ |

A.2.7 Reporting of e-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 Ipad) 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 (emergency only) | | ✓ | | | | | | ✓ |
| 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

Access to email is provided by our peri-tech services, namely IBS Schools.

These 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 a class email account to communicate with people inside 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 / 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 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 in school (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.3.2c - Videoconferencing

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

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

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

Videoconferencing is normally supervised directly by a teacher. In the event of this not being the case pupils must ask permission from the teacher before making or answering a videoconference call.

Permission for pupils to take part in video conferences is sought from parents / carers at the beginning of the pupil's time in the school (see section A.2.3 and Appendix 1). Only where permission is granted may pupils participate.

Only key administrators have access to videoconferencing administration areas.

Unique log on and password details for the educational videoconferencing services (such as the Janet booking system) are only issued to members of staff.

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 Use of web-based publication tools

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

Our school uses the public facing website (www.doddfordfirstschool.co.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.*
- Detailed calendars (including specific times of day) will not be published on the school website.
- Photographs published on the website, or elsewhere, that include pupils will be selected carefully and will comply with the following good practice guidance on the use of such images:
 - ✓ pupils' full names will not be used anywhere on a website or blog, and never in association with photographs
 - ✓ *where possible, photographs will not allow individuals to be recognised*
 - ✓ written permission from parents or carers will be obtained before photographs of pupils are published on the school/academy 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

Class 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 administrator.

User accounts and access rights can only be created by the school 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 e-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/academy systems.
- Personal email addresses, text messaging or public chat / social networking technology must not be used for these communications.

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

Section B. Infrastructure

B.1 Password security

The school's e-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 through IBS Schools, 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 **e-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: *(choose relevant response(s) below)*

- be logged in change-control logs by the person making the change
- *be reported to a second responsible person (the head teacher / ICT coordinator / 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*

All users have a responsibility to report immediately to teachers / e-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 e-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 through the Acceptable Use Agreement and through *e-safety awareness sessions / newsletter 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 e-safety coordinator.
- The e-safety coordinator checks the website content to ensure that it is appropriate for use in school.

THEN

- *If agreement is reached, the e-safety coordinator makes a request to IBS Schools Broadband Team.*
- *The Broadband helpdesk 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 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.
- 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:

- Identified members of staff (the headteacher and the ICT/ E-Safety co-ordinator) review the monitoring console captures weekly.
- Potential issues are referred to an appropriate person depending on the nature of the capture.
- Teachers are encouraged to identify in advance any word or phrase likely to be picked up regularly through innocent use (e.g. 'goddess' is captured frequently when a class is researching or creating presentations on the Egyptians) so that the word can be allowed for the period of the topic being taught.

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 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 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 the 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 Computing, PHSE and other lessons. This is regularly revisited, covering the use of ICT and new technologies both in school and beyond school.
- We use the resources on the Worcestershire E-safety website and Purplemash Scheme as a source of e-safety education resources <http://www.wes.networks.net> (e.g Hector's World at KS1 and Cyber Café and SAFE social networking at KS2).
- Learning opportunities for e-safety are built into the Computing curriculum through Purple Mash.
- Key e-safety messages will be reinforced through further input via assemblies and pastoral activities, as well as informal conversations when the opportunity arises.
- Key messages and sources of help for parents whilst children are accessing online learning platforms and generally using the internet at home will be communicated via regular newsletters.
- 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/academy.
- *In lessons where internet use is pre-planned, it is best practice that younger pupils should be guided to sites checked as suitable for their use. Processes should be in place, and known to pupils, for dealing with any unsuitable material that is found in internet searches.*
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit, encouraging pupils to discuss anything of which they are unsure and implementing the expected sanctions and/or support as necessary.
- Pupils 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 e-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 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.
- *It is expected that some staff will identify e-safety as a training need within the performance management process.*
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school/academy e-safety policy and Acceptable Use Agreements, which are signed as part of their induction
- *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 WSCB 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 those who are members of any subcommittee or group involved in ICT, e-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 e-safety governor works closely with the e-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 e-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.*
- *Parents evenings*
- *Reference to the parents materials through the Worcestershire E-Safety website (www.wes.networcs.net) and others.*

C.5 Wider community understanding

The school will offer family learning courses in e-safety so that parents and pupils can together gain a better understanding of these issues.

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.

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

Appendix 1A : Foundation Stage Acceptable User Agreement.

DODFORD FIRST SCHOOL



Every Day, a Learning Journey

Acceptable User Policy Foundation Stage



This is how we stay safe when we use computers and mobile devices:

- I will ask an adult if I want to use a 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 that I have done something wrong.
- I will tell an adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer or other equipment.
- I understand these computer rules and will do my best to keep them.

| | |
|---|--|
| Child's FULL Name: | |
| I HAVE READ THIS TO MY CHILD | |
| Parent's signature: | |
| Date: | |

DODFORD FIRST SCHOOL



Every Day, a Learning Journey

Acceptable User Policy Key Stage One



This is how to stay safe when we use computers and mobile devices:

- I will ask an adult if I want to use the computer or mobile devices
- 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 screen and tell an adult if I see something that upsets me
- I know that if I break the rules I might not be allowed to use a computer or mobile device.

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

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

Appendix 1c – Acceptable Use Agreement – pupil (KS2)

DODFORD FIRST SCHOOL



Every Day, a Learning Journey

Acceptable User Policy Key Stage Two

I understand that while I am a member of **Dodford First 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 not deliberately bypass any systems designed to keep the school 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 (especially those from the internet) on devices belonging to the school without permission.

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: | |

DODFORD FIRST SCHOOL



Every Day, a Learning Journey

Acceptable User Policy School Staff

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 e-safety in my work with young people.

For my professional and personal safety:

- I understand that the E-Safety Co-ordinator may 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 Dodford First 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 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 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) 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 e-safety policy)
- I will only use chat and social networking sites in school in accordance with the school's policies.

- I will only communicate with pupils and parents / carers using official 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 ICT 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 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 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 1e: Acceptable User Agreement Parents and Carers

DODFORD FIRST SCHOOL



Every Day, a Learning Journey

Acceptable User Policy Parents/Carers

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

This Acceptable Use Agreement is intended to ensure that:

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

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

Parents are requested to sign the permission form below to show their support of the 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 ICT systems at the 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 ICT – both in and out of the 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 ICT systems. I also understand that the school/academy cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the 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 the school/academy. 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 school website and occasionally in the public media.

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

As the parent/carer of the above pupil, I agree to the 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 at 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 our school's policy, from time to time, to publish the work of pupils by way of celebration. This includes on the internet; via the website *and on Twitter*.

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

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

Appendix 1f - Acceptable Use Agreement – community user

DODFORD FIRST SCHOOL



Every Day, a Learning Journey

Acceptable User Policy 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/academy.
- 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/academy'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 1g: Governor Acceptable User Agreement

DODFORD FIRST SCHOOL



Every Day, a Learning Journey

Acceptable User Policy – Governing Body.

For my professional and personal safety:

- I understand that the school's email system is intended only for Governing Body communication and that I will not use the system for personal or recreational use.
- I will not use my personal email for any governor related business.
- I will not disclose my email 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 through my emails, to the appropriate person.
- I will not use my governor email address to communicate matters concerning my child if I am a Parent Governor.

I will be professional in my communications and actions when using the school email system:

- 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 send sensitive data about pupils or staff through my emails.
- I understand that data protection policy requires that any information emailed will be kept private and confidential.

Governors are reminded of the importance of keeping information secure and not accessing the school email address on devices that other people have access to, and to take all reasonable steps to comply with this policy.

| | |
|----------------|--|
| Governor 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/academy 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/lrsi_report.pdf

“Guidelines on misuse of camera and video phones in school/academies”

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

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

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

<https://www.commonsemmedia.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 |
| ICT | Information and Communications Technology |
| ICT Mark | Quality standard for school/academys provided by NAACE for DfE |
| INSET | In-service Education and Training |
| IP address | The label that identifies each computer to other computers using the IP (internet protocol) |
| ISP | Internet Service Provider |
| IWF | Internet Watch Foundation |
| JANET | Provides the broadband backbone structure for Higher Education and for the National Education Network and Regional Broadband Consortia |
| KS1; KS2 | KS1 = years 1 and 2 (ages 5 to 7) KS2 = years 2 to 6 (age 7 to 11) |
| LA | Local Authority |
| LAN | Local Area Network |
| Learning platform | An online system designed to support teaching and learning in an educational setting |
| LSCB | Local Safeguarding Children Board |
| MIS | Management Information System |
| NEN | National Education Network – works with the Regional Broadband Consortia (eg WMNet) to provide the safe broadband provision to school/academys across Britain. |
| Ofcom | Office of Communications (Independent communications sector regulator) |
| Ofsted | Office for Standards in Education, Children’s Services and Skills |
| PDA | Personal Digital Assistant (handheld device) |
| PHSE | Personal, Health and Social Education |
| SRF | Self Review Framework – a tool maintained by Naace used by school/academies to evaluate the quality of their ICT provision and judge their readiness for submission for the ICTMark |
| SWGfL | South West Grid for Learning – the Regional Broadband Consortium of SW Local Authorities and recognised authority on all matters relating to 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 | | | | | | | Signature | | |
|---------------|------|----------|--------------|--|----------|----------------------|----------------------|--|--|
| Group | | | | | | | Incident Reported by | | |
| Date | Time | Incident | Action taken | | By whom? | Incident Reported by | Signature | | |
| | | | What? | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

Policy reviewed by : Nik Eggleton, April 2020

Policy agreed by Staff:

Policy agreed by Governors:

Policy to be reviewed:

Effective: immediately