|  |
| --- |
| Solihull e-safety toolkit |
| Developing an e‑safety policy  Guidance and templates for all Solihull schools and academies |
| |  |  | | --- | --- | | **Document Information** | | | Name | **[]** | | Section | **[]** | | Contact | **[]** | | Email | [[]](mailto:shalliday@solihull.gov.uk) | | Online information | [Solgrid Extranet > Path > Path] | |

[Acknowledgements 3](#_Toc380998301)

[About SWGfL/UK Safer Internet Centre 3](#_Toc380998302)

[Introduction 4](#_Toc380998303)

[Producing your schools' e-safety policy 5](#_Toc380998304)

[Using this document and associated templates 6](#_Toc380998305)

[Development, monitoring, and review of this policy 8](#_Toc380998306)

[Schedule for Development/Monitoring/Review 8](#_Toc380998307)

[Scope of the Policy 9](#_Toc380998308)

[Roles and Responsibilities 9](#_Toc380998309)

[Governors/Board of Directors 10](#_Toc380998310)

[[Headteacher/Principal] and senior leaders 10](#_Toc380998311)

[E-safety Coordinator/Officer 10](#_Toc380998312)

[Network Manager/Technical staff 11](#_Toc380998313)

[Teaching and Support Staff 12](#_Toc380998314)

[Child Protection/Safeguarding Designated Person/Officer 12](#_Toc380998315)

[E-safety Group 13](#_Toc380998316)

[Students/pupils 13](#_Toc380998317)

[Parents/Carers 14](#_Toc380998318)

[Community Users 14](#_Toc380998319)

[Policy Statements 15](#_Toc380998320)

[Education – students/pupils 15](#_Toc380998321)

[Education – parents/carers 16](#_Toc380998322)

[Education – The Wider Community 16](#_Toc380998323)

[Education & Training – Staff/Volunteers 16](#_Toc380998324)

[Training – Governors/Directors 17](#_Toc380998325)

[Technology 18](#_Toc380998326)

[Information 18](#_Toc380998327)

[Bring Your Own Device (BYOD) 20](#_Toc380998328)

[Use of digital and video images 20](#_Toc380998329)

[Data Protection 22](#_Toc380998330)

[Communications 23](#_Toc380998331)

[Social Media - Protecting Professional Identity 25](#_Toc380998332)

[Unsuitable/inappropriate activities 26](#_Toc380998333)

[User Actions 28](#_Toc380998334)

[Responding to incidents of misuse 28](#_Toc380998335)

[[school/academy] Actions & Sanctions 29](#_Toc380998336)

[Staff 31](#_Toc380998337)

[Actions/Sanctions 31](#_Toc380998338)

[Appendices 32](#_Toc380998339)

# Acknowledgements

[Say something nice about SWGfL]

SWGfL would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this School E-safety Policy Template and of the 360 degree safe E-safety Self Review Tool:

* Members of the SWGfL E-safety Group
* Avon and Somerset Police
* Representatives of SW Local Authorities
* Plymouth University Online Safety
* NEN/Regional Broadband Grids

Copyright of these Template Policies is held by SWGfL. Schools/Academies and other educational institutions are permitted free use of the Template Policies for the purposes of policy review and development. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL ([esafety@swgfl.org.uk](mailto:esafety@swgfl.org.uk)) and acknowledge its use.

Every effort has been made to ensure that the information included in this document is accurate, as at the date of publication in October 2013. However, SWGfL can not guarantee its accuracy, nor can it accept liability in respect of the use of the material.

© SWGfL 2013

# Introduction

[Get someone important?]

## Producing your schools' e-safety policy

**This guidance and the associated templates is to help schools produce an   
e‑safety policy which considers all current and relevant issues in a whole school context; that is linked to other relevant policies, such as the child protection, safeguarding, behaviour and anti-bullying policies.**

Ensuring that children and young people are able to use the internet and related communications technologies appropriately and safely is part of the wider duty of care to which all who work in schools are bound. Schools should, through their   
e‑safety policy, ensure that they meet their statutory obligations to ensure that children and young people are safe and are protected from potential harm, both within and outside school. The policy will also form part of the school's protection from other, sometimes legal, challenges related to the use of digital technologies.

In England, schools are now subject to increased scrutiny by Ofsted during inspections – following the introduction of the new framework and updated briefing documents on e‑safety[[1]](#footnote-1).

The templates suggest statements which, we think, should be essential in any school e‑safety policy that was based on good practice. In addition, there are also a range of optional statements that schools should consider; choosing those that are most suitable, given their particular circumstances.

An effective school e‑safety policy must be tailored to the needs and context of each school. Therefore, an important part of the process will be the discussion and consultation which takes place during the writing or review of the policy. This will help ensure that the policy is owned and accepted by the whole school community.

We think that that consultation in the production of this policy should involve:

* Governors or directors;
* Teaching and support staff;
* Students/pupils;
* Parents; and
* Community users and any other relevant groups.

Due to the changing nature of digital technologies, it is good practice that the school reviews the e‑safety policy annually and, if necessary, at other times. This could be where there has been a significant new development in the use of technology, where new threats have emerged or where an incident has taken place.

## Using this document and associated templates

**Given the range of optional statements offered and the guidance notes provided, this document is much longer than the resulting school policy is likely to be.**

We think that, while e-safety is a complicated and changing part of the work of a school, the policy should be concise and easily understood. Or it risks not being effective or valued and adopted by all.

|  |
| --- |
| [Guidance is shown like this] [DN as are drafting notes that tell you about particular text changes you might need to think about.]  We assume that schools that schools will remove these sections from their completed policy document, though this will be a decision for the group that produces the policy. |
| **Parts we think should be essential are in bold.** |
| Alternative terms are shown like [this/that]  The templates use a number of alternative terms, like   * [headteacher/principal]; * [governors/directors]; * [students/pupils]; or * [local authority/other responsible body].   Each time these appear in brackets. Schools and academies will need to choose which term is relevant and delete the other along with the brackets. |
| *Optional sections in the template are written in italics and schools would wish to think about whether or not to include that section or statement in their completed policy at all.* |
| We have prepared this information using standard conventions to try and make it simpler for people with visual impairments to read. As examples, we use as few capital letters as possible on titles, and the whole document is set using a minimum of a12pt font size for body text. Obviously, schools may wish to change this to suit their own style conventions. |

The first part of this document (approximately 20 pages) provides a template for an overall e-safety policy for the school. The appendices contain a more detailed and more specific policy templates and agreement forms. It will be for schools/academies to decide which of these documents they chose to amend and adopt.

The pages that follow contain the suggested wording for your overall school e‑safety safety policy.

|  |
| --- |
| Solihull e-safety toolkit |
| [School name]  [Draft] E-safety policy |
| |  |  | | --- | --- | | **Document Information** | | | Filename | **[DN insert filename]** | | Date | **[DN insert date adopted by governing body]** | | Contact name | **[DN insert name of responsible person]** | | Email | **[DN insert name of responsible person]** | | Notes | **[DN insert notes pertaining to this version]** | |

2

## Development, monitoring, and review of this policy

4

This e‑safety policy has been developed by a [working group/committee] [DN or insert name of group] made up of: [ DN delete/add as relevant]

* [Headteacher/principal/senior leaders]
* [E-safety officer/coordinator]
* [Staff – including teachers, support staff and technical staff]
* [Governors/board of directors]
* [Parents and carers]
* [Community users]

Consultation with the whole school community has taken place through a range of formal and informal meetings. [DN you might want to expand with some detail]

## Schedule for Development/Monitoring/Review

5

|  |  |
| --- | --- |
| This e‑safety policy was approved by the [board of directors/governing body/governors subcommittee] on | [DN insert date] |
| The implementation of this e‑safety policy will be monitored by the | [DN insert name of group/individual] [suggested groups – e-safety coordinator/officer/committee, senior leadership team] |
| Monitoring will take place at regular intervals and will take place at least | [DN insert time period]  [suggested to be at least once a year] |
| The [board of directors/governing body/governors subcommittee] will receive a report on the implementation of the e‑safety policy generated by the monitoring group *which will include anonymous details of e‑safety incidents* | [DN insert time period]  [suggested to be at least once a year] |
| The e-safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e‑safety or incidents that have taken place. The next anticipated review date will be | [DN insert date] |

The school will monitor the impact of the policy using: [DN delete/add as relevant]

* *Logs of reported incidents*
* *Monitoring logs of internet activity (including sites visited)*
* *Internal monitoring data for network activity*
* *Surveys/questionnaires of* 
  + *students/pupils*
  + *parents/carers*
  + *staff*

6

## Scope of the Policy

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

The Education and Inspections Act 2006 empowers [headteachers/principals] to such extent as is reasonable, to regulate the behaviour of [students/pupils] when they are off the [[school/academy] site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e‑safety incidents covered by this policy, which may take place outside of the [school/academy], but is linked to membership of the [school/academy]. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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

## Roles and Responsibilities

7

The following section outlines the e‑safety roles and responsibilities of individuals and groups within the [school/academy].

[In a small [school/academy] some of the roles described below may be combined, though it is important to ensure that there is sufficient separation of responsibility should this be the case.]

### [Governors/Board of Directors]

[Governors/Directors] are responsible for the approval of the E-safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the [Governors/Directors/Sub Committee] receiving regular information about e‑safety incidents and monitoring reports. A member of the [Governors/Directors/Sub Committee] has taken on the role of E-safety [Governor/Director].

[DN it is suggested that the role may be combined with that of the Child Protection/Safeguarding Governor.]

The role of the E-safety [Governor/Director] will include:

* regular meetings with the E-safety [Co-ordinator/Officer]
* regular monitoring of e‑safety incident logs
* regular monitoring of filtering/change control logs
* reporting to relevant [Governors/Board/committee/meeting]

### [Headteacher/Principal] and senior leaders

* The [Headteacher/Principal] has a duty of care for ensuring the safety (including e‑safety) of members of the school community, though the day to day responsibility for e‑safety will be delegated to the *E-safety Co-ordinator/Officer*.
* The Headteacher and (at least) another member of the Senior Leadership Team/Senior Management Team should be aware of the procedures to be followed in the event of a serious e‑safety allegation being made against a member of staff. (see flow chart on dealing with e‑safety incidents – included in a later section – “Responding to incidents of misuse” and relevant *Local Authority HR/other relevant body* disciplinary procedures).
* The Headteacher/Principal/Senior Leaders are responsible for ensuring that the E-safety Coordinator/Officer and other relevant staff receive suitable training to enable them to carry out their e‑safety roles and to train other colleagues, as relevant.
* The Headteacher/Principal/Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e‑safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.   
    
  [DN The [school/academy] will need to describe this and may wish to involve the Local Authority/other responsible body in this process]
* The Senior Leadership Team/Senior Management Team will receive regular monitoring reports from the E-safety Co-ordinator/Officer.

### E-safety coordinator/officer

[DN It is strongly recommended that each school should have a named member of staff with a day to day responsibility for e‑safety, some schools may choose to combine this with the Child Protection/Safeguarding Officer role. Schools may choose to appoint a person with a child welfare background, preferably with good knowledge and understanding of the new technologies, rather than a technical member of staff – but this will be the choice of the school]

The E-safety Coordinator/Officer

* 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 taking place.
* provides training and advice for staff
* liaises with the Local Authority/relevant body
* liaises with school technical staff
* receives reports of e‑safety incidents and creates a log of incidents to inform future e‑safety developments, (Examples of suitable log sheets may be found later in this document). meets regularly with E-safety *Governor/Director* to discuss current issues, review incident logs and filtering/change control logs
* attends relevant meeting/committee of *Governors/Directors*
* reports regularly to Senior Leadership Team

[DN The school will need to decide how these incidents will be dealt with and whether the investigation/action/sanctions will be the responsibility of the E-safety Co-ordinator/Officer or another member of staff eg Headteacher/Principal/Senior Leader/Safeguarding Officer/Class teacher/Head of Year etc.)

### Network manager/technical staff

[DN if the [school/academy] has a managed ICT service provided by an outside contractor, it is the responsibility of the [school/academy] to ensure that the managed service provider carries out all the e‑safety measures that would otherwise be the responsibility of the school technical staff, as suggested below. It is also important that the managed service provider is fully aware of the [school/academy] e‑safety policy and procedures.]

The Network Manager/Technical Staff/Co-ordinator for ICT/Computing is responsible for ensuring:

* that the *school’s/academy’s* technical infrastructure is secure and is not open to misuse or malicious attack
* that the [school/academy] meets required e‑safety technical requirements and any *Local Authority/other relevant body* E-safety Policy/Guidance that may apply.
* that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
* the filtering policy (if it has one), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person (see appendix “Technical Security Policy Template” for good practice)
* that they keep up to date with e‑safety technical information in order to effectively carry out their e‑safety role and to inform and update others as relevant
* that the use of the network/internet/Virtual Learning Environment /remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher/Principal/Senior Leader; E-safety Coordinator/Officer (insert others as relevant) for investigation/action/sanction
* that monitoring software/systems are implemented and updated as agreed in [school/academy] policies

### Teaching and support staff

Teaching and support staff are responsible for ensuring that:

* they have an up to date awareness of e‑safety matters and of the current [school/academy] e‑safety policy and practices
* they have read, understood and signed the Staff Acceptable Use Policy/Agreement (AUP)
* they report any suspected misuse or problem to the Headteacher/Principal/Senior Leader ; E-safety Coordinator/Officer [DN insert others as relevant] for investigation/action/sanction
* all digital communications with students/pupils/parents/carers should be on a professional level *and only carried out using official school systems*
* e‑safety issues are embedded in all aspects of the curriculum and other activities
* students/pupils understand and follow the e‑safety and acceptable use policies
* students/pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
* they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
* in lessons where internet use is pre-planned students/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

### [Child protection/safeguarding designated person/officer]

The [child protection/safeguarding designated person/officer] should be trained in e‑safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

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

[DN it is important to emphasise that these are child protection issues, not technical issues, simply that the technology provides additional means for child protection issues to develop. Some schools may choose to combine the role of Child Protection Officer/Safeguarding Officer and E-safety Officer]

### E-safety group

The e-safety group provides a consultative group that has wide representation from the [school/academy] community, with responsibility for issues regarding e‑safety and the monitoring the e‑safety policy including the impact of initiatives. Depending on the size or structure of the [school/academy] this committee may be part of the safeguarding group. The group will also be responsible for regular reporting to the [Governing Body/Directors].

Members of the E-safety Group (or other relevant group) will assist the E-safety Coordinator/Officer (or other relevant person, as above) with:

* the production/review/monitoring of the school e‑safety policy/documents
* the production/review/monitoring of the school filtering policy (if the school chooses to have one) and requests for filtering changes
* mapping andreviewing the e‑safety curricular provision – ensuring relevance, breadth and progression
* monitoring network/internet/incident logs
* consulting stakeholders – including parents/carers and the students/pupils about the e‑safety provision
* monitoring improvement actions identified through use of the 360 degree safe self review tool

[Schools/academies] will need to decide the membership of the e‑safety group. It is recommended that the group should include representation from students/pupils and parents/carers).

An e-safety group *terms of reference* template can be found in the appendices

### Students/pupils

Students/pupils:

* are responsible for using the [school/academy] digital technology systems in accordance with the student/pupil acceptable use policy
* have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
* need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
* will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on cyber-bullying
* should understand the importance of adopting good e‑safety practice when using digital technologies out of school and realise that the [school’s/academy’s] e-safety policy covers their actions out of school, if related to their membership of the school

### Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The [school/academy] will take every opportunity to help parents understand these issues through [*parents’ evenings, newsletters, letters, website/VLE and information about national/local e‑safety campaigns/literature.* Parents and carers will be encouraged to support the [school/academy] in promoting good e‑safety practice and to follow guidelines on the appropriate use of:

* digital and video images taken at school events
* access to parents’ sections of the website/VLE and on-line student/pupil records
* their children’s personal devices in the [school/academy] (where this is allowed)

### Community Users

Community Users who access school systems/website/VLE as part of the wider [school/academy] provision will be expected to sign a *community user AUP* before being provided with access to school systems. [A community users acceptable use agreement template can be found in the appendices.]

11

## Policy Statements

### Education – students/pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating *students/pupils* to take a responsible approach. The education of *students/pupils* in e‑safety is therefore an essential part of the school’s e‑safety provision. Children and young people need the help and support of the school to recognise and avoid e‑safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum and staff should reinforce e‑safety messages across the curriculum. The e‑safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

[DN statements will need to be adapted, depending on [school/academy] structure and the age of the students/pupils]

* [a planned e‑safety curriculum should be provided as part of computing/PHSE/other lessons and should be regularly revisited]
* [key e‑safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities]
* [students/pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information]
* [students/pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet]
* [students/pupils should be helped to understand the need for the student/pupil AUA and encouraged to adopt safe and responsible use both within and outside school]
* [staff should act as good role models in their use of digital technologies the internet and mobile devices]
* [in lessons where internet use is pre-planned, it is best practice that students/pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches]
* [where students/pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit]
* [it is accepted that from time to time, for good educational reasons, students may need to research topics (as examples, racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the technical staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need]

### Education – parents/carers

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/regulation of the children’s on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through: [DN select/delete as appropriate]

* Curriculum activities
* Letters, newsletters, web site, VLE
* Parents/Carers evenings/sessions
* High profile events/campaigns eg Safer Internet Day
* *Reference to the relevant web sites/publications eg [add]*

### Education – The Wider Community

The [school/academy] will provide opportunities for local community groups/members of the community to gain from the school’s/academy’s e‑safety knowledge and experience. This may be offered through the following:

* Providing family learning courses in use of new digital technologies, digital literacy and e‑safety
* E-safety messages targeted towards grandparents and other relatives as well as parents.
* The [school/academy] website will provide e‑safety information for the wider community
* Supporting community groups eg Early Years settings, childminders, youth/sports/voluntary groups to enhance their e‑safety provision [possibly supporting the group in the use of Online Compass, an online safety self-review tool - [www.onlinecompass.org.uk](http://www.onlinecompass.org.uk) ]

### Education & Training – Staff/Volunteers

It is essential that all staff receive e‑safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows: [select/delete as appropriate]

* A planned programme of formal e‑safety training will be made available to staff. This will be regularly updated and reinforced. 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 e‑safety policy and Acceptable Use Agreements.
* The E-safety Coordinator/Officer (or other nominated person) will receive regular updates through attendance at external training events (eg from SWGfL/LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations.
* This E-safety policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days.
* The E-safety Coordinator/Officer (or other nominated person) will provide advice/guidance/training to individuals as required.

### Training – Governors/Directors

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

* Attendance at training provided by the Local Authority/National Governors Association /or other relevant organisation (eg SWGfL).
* Participation in school training/information sessions for staff or parents (this may include attendance at assemblies/lessons).

## Technology

## Information

[If the [school/academy] has a managed ICT service provided by an outside contractor, it is the responsibility of the school to ensure that the managed service provider carries out all the e-safety measures that would otherwise be the responsibility of the school, as suggested below. It is also important that the managed service provider is fully aware of the school/academy e-safety policy/ acceptable use agreements. The school should also check their local authority/other relevant body policies on these technical issues.]

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

[Schools/academies will have very different technical infrastructures and differing views as to how these technical issues will be handled – it is therefore essential that this section is fully discussed by a wide range of staff – technical, educational and administrative staff before these statements are agreed and added to the policy]

* A more detailed Technical Security Template Policy can be found in the appendix.
* [school/academy] technical systems will be managed in ways that ensure that the [school/academy] meets recommended technical requirements (these may be outlined in Local Authority/other relevant body policy and guidance).
* There will be regular reviews and audits of the safety and security of school academy technical systems
* Servers, wireless systems and cabling must be securely located and physical access restricted
* All users will have clearly defined access rights to [school/academy] technical systems and devices.
* All users (at KS2 and above) will be provided with a username and secure password by [DN insert name or title]who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password every (insert period). [Schools/Academies may choose to use group or class log-ons and passwords for KS1 and below, but need to be aware of the associated risks – see appendix]
* Administrator passwords for the [school/academy] ICT system, used by the Network Manager (or other person) must also be available to the [Headteacher/Principal] or other nominated senior leader and kept in a secure place (eg school safe). They must be sealed in a signed envelope that is only to be opened when necessary
* [DN Insert name or role] is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)

Internet access is filtered for all users. [DN insert details of filtration methodology] There is a clear process in place to deal with requests for filtering changes (see appendix for more details)

* The school has provided enhanced/differentiated user-level filtering(allowing different filtering levels for different ages/stages and different groups of users – staff/pupils/students etc)
* [school/academy] technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement. [DN schools may wish to add details of the monitoring programmes that are used.]
* An appropriate system is in place [DN to be described] for users to report any actual/potential technical incident/security breach to the relevant person, as agreed).
* Appropriate security measures are in place [DN schools may wish to provide more detail] to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
* An agreed policy is in place [DN to be described] for the provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto the school systems.
* An agreed policy is in place [DN to be described] regarding the extent of personal use that users (staff/students/pupils/community users) and their family members are allowed on school devices that may be used out of school.
* An agreed policy is in place [DN to be described] that allows staff to/forbids staff from downloading executable files and installing programmes on school devices.
* An agreed policy is in place (to be described) regarding the use of removable media (eg memory sticks/CDs/DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. (see School Personal Data Policy Template in the appendix for further detail)

### Bring Your Own Device (BYOD)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of e‑safety considerations for BYOD that need to be reviewed prior to implementing such a policy. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring. This list is not exhaustive and a BYOD policy should be in place and reference made within all relevant policies. (see appendix for a more detailed BYOD Policy Template)

* The school has a set of clear expectations and responsibilities for all users
* The school adheres to the Data Protection Act principles
* All users are provided with and accept the Acceptable Use Agreement
* All network systems are secure and access for users is differentiated
* Where possible these devices will be covered by the school’s/academy’s normal filtering systems, while being used on the premises
* All users will use their username and password and keep this safe
* Mandatory training is undertaken for all staff
* Students/Pupils receive training and guidance on the use of personal devices
* Regular audits and monitoring of usage will take place to ensure compliance
* Any device loss, theft, change of ownership of the device will be reported as in the BYOD policy
* Any user leaving the school will follow the process outlined within the BYOD policy

### Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students/pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students/pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm: [DN select/delete as appropriate]

* When using digital images, staff should inform and educate students/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 eg on social networking sites.
* In accordance with guidance from the Information Commissioner’s Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone’s privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other *students/pupils* in the digital/video images.
* Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
* Care should be taken when taking digital/video images that students/pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
* Students/pupils must not take, use, share, publish or distribute images of others without their permission
* Photographs published on the website, or elsewhere that include students/pupils will be selected carefully and will comply with good practice guidance on the use of such images.
* Students’/Pupils’ full names will not be used anywhere on a website or blog, particularly in association with photographs.
* Written permission from parents or carers will be obtained before photographs of students/pupils are published on the school website (may be covered as part of the AUA signed by parents or carers at the start of the year - see **Parents/Carers Acceptable Use Agreement** in the appendix).
* Student’s/Pupil’s work can only be published with the permission of the student/pupil and parents or carers.

### Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

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

[DN Following a number of “high profile” losses of personal data by public organisations, schools are likely to be subject to greater scrutiny in their care and use of personal data. A School Personal Data template is available in the appendices to this document. (Schools/Academies should review and amend this appendix, if they wish to adopt it. Schools/Academies should also ensure that they take account of relevant policies and guidance provided by local authorities or other relevant bodies.]

The [school/academy] must ensure that:

* it will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
* every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
* all personal data will be fairly obtained in accordance with the “Privacy Notice” and lawfully processed in accordance with the “Conditions for Processing”. (see **Privacy Notice** section in the appendix)
* it has a Data Protection Policy (see appendix for template policy)
* it is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
* responsible persons are appointed/identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
* appropriate risk assessments are carried out
* It has clear and understood arrangements for the security, storage and transfer of personal data
* data subjects have rights of access and there are clear procedures for this to be obtained
* there are clear and understood policies and routines for the deletion and disposal of data
* there is a policy for reporting, logging, managing and recovering from information risk incidents
* there are clear data protection clauses in all contracts where personal data may be passed to third parties
* there are clear policies about the use of cloud storage/cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner’s Office

Staff must ensure that they: [DN schools/academies may wish to include more detail about their own data/password/encryption/secure transfer processes.]

* follow the [school’s/academy’s] data protection policies
* at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
* use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.
* transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

* the data must be encrypted and password protected
* the device must be password protected. Please note that many memory sticks/cards and other mobile devices cannot be password protected.
* the device must offer approved virus and malware checking software

16

* the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

[The school will need to set its own policy as to whether data storage on removal media is allowed, even if encrypted – some organisations do not allow storage of personal data on removable devices.]

The Personal Data Handling Policy Template in the appendix provides more detailed guidance on the school’s/academy’s responsibilities and on good practice.

### Communications

[This is an area of rapidly developing technologies and uses. Schools will need to discuss and agree how they intend to implement and use these technologies eg few schools allow students/pupils to use mobile phones in lessons, while others recognise their educational potential and allow their use. This section may also be influenced by the age of the students/pupils. The table has been left blank for school to choose its own responses.]

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

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Communication Technologies** | **Staff & other adults** | | | | **Students/Pupils** | | | | |
|  | Allowed | Allowed at certain times | Allowed for selected staff | Not allowed | Allowed | Allowed at certain times | Allowed with staff permission | Not allowed |
| Mobile phones may be brought to school |  |  |  |  |  |  |  |  |
| Use of mobile phones in lessons |  |  |  |  |  |  |  |  |
| Use of mobile phones in social time |  |  |  |  |  |  |  |  |
| Taking photos on mobile phones/cameras |  |  |  |  |  |  |  |  |
| Use of other mobile devices (as examples tablets, gaming devices) |  |  |  |  |  |  |  |  |
| Use of personal email addresses in school, or on school network |  |  |  |  |  |  |  |  |
| Use of school email for personal emails |  |  |  |  |  |  |  |  |
| Use of messaging apps |  |  |  |  |  |  |  |  |
| Use of social media |  |  |  |  |  |  |  |  |
| Use of blogs |  |  |  |  |  |  |  |  |

[The school may also wish to add some of the following policy statements about the use of communications technologies, in place of, or in addition to the above table.]

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

* The official [school/academy] email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
* Staff and students/pupils should therefore use only the [school/academy] email service to communicate with others when in school, or on [school/academy] systems (eg by remote access).
* Users must immediately report, to the nominated person – in accordance with the [school/academy] policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
* Any digital communication between staff and students/pupils or parents/carers (email, chat, VLE 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 social media must not be used for these communications.*
* Whole class/group email addresses may be used at KS1, while students/pupils at KS2 and above will be provided with individual [school/academy] email addresses for educational use. [Schools/academies might choose to use group or class email addresses for younger age groups at FKS or KS1]
* Students/pupils should be taught about e‑safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
* Personal information should not be posted on the [school/academy] website and only official email addresses should be used to identify members of staff.

### Social Media - Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of pupils, the school and the individual when publishing any material online. Expectations for teachers’ professional conduct are set out in ‘Teachers Standards 2012’. While, Ofsted’s e‑safety framework 2012, reviews how a school protects and educates staff and pupils in their use of technology, including what measures would be expected to be in place to intervene and support should a particular issue arise.]

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the [school/academy] or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

* Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
* Clear reporting guidance, including responsibilities, procedures and sanctions
* Risk assessment, including legal risk
* School staff should ensure that:
* No reference should be made in social media to students/pupils, parents/carers or school staff
* They do not engage in online discussion on personal matters relating to members of the school community
* Personal opinions should not be attributed to the *school /academy* or local authority
* Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The *school’s/academy’s* use of social media for professional purposes will be checked regularly by the senior risk officer and e‑safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies

### Unsuitable/inappropriate activities

Some internet activity eg accessing child abuse images or distributing racist material is illegal and would obviously be banned from [school/academy] and all other technical systems. Other activities eg cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

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

| **Communication Technologies** | | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
| --- | --- | --- | --- | --- | --- | --- |
| Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to: | Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978 |  |  |  |  | ⚫ |
| Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003. |  |  |  |  | ⚫ |
| Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008 |  |  |  |  | ⚫ |
|  | criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986 |  |  |  |  | ⚫ |
| pornography |  |  |  | ⚫ |  |
| promotion of any kind of discrimination |  |  |  | ⚫ |  |
| threatening behaviour, including promotion of physical violence or mental harm |  |  |  | ⚫ |  |
| any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute |  |  |  | ⚫ |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| Using school systems to run a private business | |  |  |  | ⚫ |  |
| Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the [school/academy] | |  |  |  | ⚫ |  |
| Infringing copyright | |  |  |  | ⚫ |  |
| Revealing or publicising confidential or proprietary information (eg financial/personal information, databases, computer/network access codes and passwords) | |  |  |  | ⚫ |  |
| Creating or propagating computer viruses or other harmful files | |  |  |  | ⚫ |  |
| Unfair usage (downloading/uploading large files that hinders others in their use of the internet) | |  |  |  | ⚫ |  |
| On-line gaming (educational) | |  |  |  |  |  |
| On-line gaming (non-educational) | |  |  |  |  |  |
| On-line gambling | |  |  |  |  |  |
| On-line shopping/commerce | |  |  |  |  |  |
| File sharing | |  |  |  |  |  |

[The [school/academy] should agree its own responses and place the ticks in the relevant columns, in the table above. They may also wish to add additional text to the column(s) on the left to clarify issues. The last section of the table has been left blank for *schools/academies* to decide their own responses]

### Responding to incidents of misuse

This guidance is intended for use when staff need 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 involve illegal or inappropriate activities (see “User Actions” above).

#### Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.

[Insert link to Solihull incident flowchart]

#### Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow [school/academy] policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

* 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. 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

adult material which potentially breaches the Obscene Publications Act

criminally racist material

other criminal conduct, activity or materials

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the [school/academy] and 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.

### [School/Academy] actions and sanctions

It is more likely that the [school/academy] will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the 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: [DN the [school/academy] will need to agree upon its own responses and place the ticks in the relevant columns. They may also wish to add additional text to the column(s) on the left to clarify issues. Schools/academies have found it useful to use the charts below at staff meetings/training sessions].

| **Communication Technologies** | **Actions/Sanctions** | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Warning | Removal of network/internet access rights | Further sanction |(like detention or exclusion) | Inform parents/carers | Refer to technical support staff for action re filtering/security etc | Refer to class teacher/tutor | Refer to Head of Department/Head of Year/other | Refer to Headteacher/Principal | Refer to Police |
| 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 mobile device |  |  |  |  |  |  |  |  |  |
| Unauthorised use of social media/ messaging apps/personal email |  |  |  |  |  |  |  |  |  |
| Unauthorised downloading or uploading of files |  |  |  |  |  |  |  |  |  |
| Allowing others to access [school/academy] network by sharing username and passwords |  |  |  |  |  |  |  |  |  |
| Attempting to access or accessing the [school/academy] network, using another student’s /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 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/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  21 |  |  |  |  |  |  |  |  |  |

### Appendices

Copies of the more detailed template policies and agreements, contained in the appendix, can be downloaded from:

[Insert list of appendices]

[Insert list of suggested appendices]

### Change control

This policy is subject tochnage control. Major revisions are listed here.

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Owner** | **Comments** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. <http://www.ofsted.gov.uk/resources/briefings-and-information-for-use-during-inspections-of-maintained-schools-and-academies>. [↑](#footnote-ref-1)