# POLICY

# Online Safety

SEPTEMBER 2022

Review 2025


**Assunnah Primary School**

565A High Road | London | N17 6SB

T: 0208 350 0592

E: admin@assunnahschool.co.uk
W: www.assunnahschool.co.uk

School Manager: Mohamed Yusuf
Head Teacher: Hoden Yussuf

# Development / Monitoring / Review of this Policy

This Online Safety policy has been developed by senior school leaders and school community made up of:

- Headteacher / / Senior Leaders
- Staff – including Teachers, Support Staff, Technical staff
- Proprietor/s
- Parents and Carers
- Community users

Consultation with the whole school has taken place through a range of formal and informal meetings.

# Schedule for Development / Monitoring / Review

| | |
|---|---|
| This Online Safety policy was approved by the Proprietors | *September 2023* |
| The implementation of this Online Safety policy will be monitored by the Head teacher and Deputy Head teacher(DSL). | *xxx* |
| Monitoring will take place at regular intervals: | *Monthly-separate file* |
| The Proprietor and the senior leaders will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals: | *As and when necessary* |
| The Online 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 online safety or incidents that have taken place. The next anticipated review date will be: | *September 2024* |
| Should serious online safety incidents take place, the following external persons / agencies should be informed: | |

The school will monitor the impact of the policy using:

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

# Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteacher/s to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the *school* site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other Online Safety incidents covered by this policy, which may take place outside of the *school*, but is linked to membership of the school. 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.

Assunnah Primary School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school.

# Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the *school*

# Proprietors:

*Proprietors* are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Proprietors receiving regular information about online safety incidents and monitoring reports.one of the Proprietors has taken on the role of *Online Safety officer and is combined with the role of the schools safeguarding officer. The* role of the Online Safety *officer* will include:

- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant meeting
- keeping up2date with legislations relating to safeguarding and e-safety.

# Headteacher and Senior Leaders:

- The *Headteacher* has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the *Online Safety Co-ordinator (Mrs Xxx).*
- 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 online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant *Local Authority HR / other relevant body* disciplinary procedures).
- *The Headteacher/Senior Leaders are responsible for ensuring that the Online Safety Coordinator / Officer and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.*
- *The Headteacher / 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 online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.*
- *The Senior Leadership Team / Senior Management Team will receive regular monitoring reports from the Online Safety Co-ordinator / Officer.*

# Network Manager / Technical staff:

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

- **that the *school's* technical infrastructure is secure and is not open to misuse or malicious attack**
- **that the *school* meets required online safety technical requirements and any *Local Authority* Online 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**

- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the *network / internet / Learning Platform / remote access / email* is regularly monitored in order that any misuse / attempted misuse can be reported to the *Headteacher Ms **Hodan Yususf*** for investigation / action / sanction
- *that monitoring software / systems are implemented and updated as agreed in school policies*

## Teaching and Support Staff

Are responsible for ensuring that:

- **they have an up to date awareness of online safety matters and of the current *school* Online 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 / / Senior Leader; Online Safety Coordinator / Officer xxx* 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***
- online safety issues are embedded in all aspects of the curriculum and other activities
- students / pupils understand and follow the Online Safety Policy 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*

## Designated Safeguarding Lead / Designated Person / Officer

Should be trained in Online 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

## Students / Pupils:

- **are responsible for using the *school* digital technology systems in accordance with the Student / Pupil Acceptable Use Agreement**
- 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 online safety practice when using digital technologies out of school and realise that the *school's* Online 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* will take every opportunity to help parents understand these issues through *parents' evenings, newsletters, letters, website / Learning Platform and information about national / local online safety campaigns / literature.* Parents and carers will be encouraged to support the *school* in promoting good online 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 / Learning Platform and on-line student / pupil records
- their children's personal devices in the school (where this is allowed)

# Policy Statements

## Education – Students / Pupils

Curriculum Input: The school ensures that pupils are aware of safeguarding through:

- The school curriculum that is designed carefully to become a model of prevention. Providing opportunities for feedback. The content of the curriculum, which includes teaching about online safety, safe relationships and personal resilience is embedded throughout the whole school curriculum and is interwoven.
- The school ethos, The Spirit of the School, which promotes a positive, supportive and secure environment and gives pupils a sense of being valued.
- The school behaviour policy, which is aimed at supporting vulnerable pupils in the school.
- Liaison with other agencies that support the pupil such as Social Care, Child and Adult Mental Health Service, Education Welfare Service and Educational Psychology service, attending case conferences where necessary.

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 online safety is therefore an essential part of Assunnah Primary school's online safety provision. Children need the help and support of the school to recognise and avoid online safety risks and build their resilience.
Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:)

- A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited this is done during the first week within a thematic week on 'SAFETY WEEK'
- Key online 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 supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- *Students / pupils should be helped to understand the need for the student / pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school / academy.*
- *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, students / pupils are always 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 remain vigilant in monitoring the content of the websites where they visit.*
- *It is accepted that from time to time, for good educational reasons, students may need to research topics (eg 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 to the head teacher.*

# Education – Parents / Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / 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.
At Assunnah Primary School we will seek to provide information and awareness to parents and carers through:

- *Letters, newsletters, web site*
- *Parents / Carers evenings / sessions*
- *High profile events / campaigns e.g. Safer Internet Day*
- *Reference to the relevant web sites / publications* Education – The Wider Community

The school will provide opportunities for local community groups / members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- *Providing family learning courses in use of new digital technologies, digital literacy and online safety*
- *Online safety messages targeted towards grandparents and other relatives as well as parents.*
- *The school / academy website will provide online safety information for the wider community*
- *Supporting community groups e.g. Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their Online Safety provision*

# Education & Training – Staff / Volunteers

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

- **A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced during INSETS and meetings.**
- **All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school internet Safety Policy and Acceptable Use Agreements.**
- *It is expected that some staff will identify online safety as a training need within the performance management process.*

- *The Online Safety Coordinator (xxx) will receive regular updates through attendance at external training events e.g. Haringey LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.*
- *This Online Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.*
- *The Online Safety Coordinator (xxx) will provide advice / guidance / training to individuals as required.*

# Training – Proprietor

**The Proprietor should take part in online safety training / awareness sessions**, with particular importance for those who are members of any subcommittee / group involved in technology / online safety / health and safety /safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation e.g. Haringey children services
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

# Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school 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 online safety responsibilities:

- **School technical systems will be managed in ways that ensure that it meets recommended technical requirements**
- **There will be regular reviews and audits of the safety and security of school technical systems can be found within the safeguarding audit**
- **Servers, wireless systems and cabling must be securely located and physical access restricted**
- **All users will have clearly defined access rights to school technical systems and devices.**
- The "master / administrator" passwords for the school / academy ICT system, used by the Network Manager (or other person) must also be available to the *Headteacher /* or other nominated senior leader and kept in a secure place e.g. school.
- Xxx (School Administrator) 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
- **Internet access is filtered for all users.** Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored
- **Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet**
- *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 technical staff regularly monitors and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.* Pupils have no access to computers or laptops without the supervision of an adult staff present. All laptops are kept locked in the cupboard and is kept in the a safe locked location. Children are never left unattended when access to computer is given in class. Scheduled times are allocated on the weekly class timetable for the computing lessons. All staff are reminded regularly of the dangers present if children are left unattended with access to internet. Pupils will be regularly reminded of the dangers and safe use of ICT, E safety will be regularly mentioned to pupils throughout the academic year.

- *An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed). Regular monitoring scheduled and unscheduled is undertaken by senior leaders, through training and regular meetings staff are reminded the responsibility and accountability of safe practice amongst students staff and school community.*
- Appropriate security measures are in place safeguarding officer will make random checks by physically testing keywords to ensure 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 provided to the school by BT.
- All temporary staff will need to read school internet and safeguarding policy for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- *An agreed policy is in place 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 that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.*
- *An agreed policy is in place regarding the use of removable media (e.g. 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****.*

# Filtering and Monitoring

- *Currently the school has BT Broadband Package which comes with a filtering package. Any future internet provider will also be provided with a filtering package.*
- *The school mainly uses the Sophos firewall as it's main filter for all web traffic*
- *The school additionally filters web traffic through both the Microsoft Defender – Advanced Threat Protection Web Filtering.*
- *Web traffic is monitored through the use of the reporting feature from the Microsoft Defender portal and the reporting feature from Sophos Firewall.*
- *The school periodically runs the test filtering tool provided from the SWGFL website: http://testfiltering.com*
- *The following areas will be filtered and monitored through the use of allowed or blocked web trafiic policies:*
- *Tables below show our standard Web Filtering policies and categories for various user groups:* **Admin, Teaching Staff and Students**

**Admin Staff Filtering**

| | | |
|---|---|---|
| ☑ 1. Violence/Hate/Racism | ☐ 23. Government | ☐ 45. Travel |
| ☑ 2. Intimate Apparel/Swimsuit | ☐ 24. Military | ☐ 46. Vehicles |
| ☑ 3. Nudism | ☐ 25. Political/Advocacy Groups | ☐ 47. Humor/Jokes |
| ☑ 4. Pornography | ☐ 26. Health | ☐ 48. Multimedia |
| ☑ 5. Weapons | ☐ 27. Information Technology/Computers | ☐ 49. Freeware/Software Downloads |
| ☑ 6. Adult/Mature Content | ☐ 28. Hacking/Proxy Avoidance Systems | ☐ 50. Pay to Surf Sites |
| ☑ 7. Cult/Occult | ☐ 29. Search Engines and Portals | ☐ 51. N/A |
| ☑ 8. Drugs/Illegal Drugs | ☐ 30. E-Mail | ☐ 52. N/A |
| ☐ 9. Illegal Skills/Questionable Skills | ☐ 31. Web Communications | ☐ 53. Kid Friendly |
| ☐ 10. Sex Education | ☐ 32. Job Search | ☐ 54. Advertisement |
| ☑ 11. Gambling | ☐ 33. News and Media | ☐ 55. Web Hosting |
| ☐ 12. Alcohol/Tobacco | ☐ 34. Personals and Dating | ☐ 56. Other |
| ☐ 13. Chat/Instant Messaging (IM) | ☐ 35. Usenet News Groups | ☐ 57. Internet Watch Foundation CAIC |
| ☐ 14. Arts/Entertainment | ☐ 36. Reference | ☐ 58. Social Networking |
| ☐ 15. Business and Economy | ☐ 37. Religion | ☐ 59. Malware |
| ☐ 16. Abortion/Advocacy Groups | ☐ 38. Shopping | ☐ 60. N/A |
| ☐ 17. Education | ☐ 39. Internet Auctions | ☐ 61. N/A |
| ☐ 18. N/A | ☐ 40. Real Estate | ☐ 62. N/A |
| ☐ 19. Cultural Institutions | ☐ 41. Society and Lifestyle | ☐ 63. N/A |
| ☐ 20. Online Banking | ☐ 42. Gay and Lesbian Issues | ☐ 64. Not Rated |
| ☐ 21. Online Brokerage and Trading | ☐ 43. Restaurants and Dining | |
| ☐ 22. Games | ☐ 44. Sports/Recreation | |

## Teaching Staff Filtering

| | | |
|---|---|---|
| ☑ 1. Violence/Hate/Racism | ☐ 23. Government | ☐ 45. Travel |
| ☑ 2. Intimate Apparel/Swimsuit | ☐ 24. Military | ☐ 46. Vehicles |
| ☑ 3. Nudism | ☐ 25. Political/Advocacy Groups | ☐ 47. Humor/Jokes |
| ☑ 4. Pornography | ☐ 26. Health | ☐ 48. Multimedia |
| ☑ 5. Weapons | ☐ 27. Information Technology/Computers | ☐ 49. Freeware/Software Downloads |
| ☑ 6. Adult/Mature Content | ☑ 28. Hacking/Proxy Avoidance Systems | ☐ 50. Pay to Surf Sites |
| ☑ 7. Cult/Occult | ☐ 29. Search Engines and Portals | ☐ 51. N/A |
| ☑ 8. Drugs/Illegal Drugs | ☐ 30. E-Mail | ☐ 52. N/A |
| ☑ 9. Illegal Skills/Questionable Skills | ☐ 31. Web Communications | ☐ 53. Kid Friendly |
| ☐ 10. Sex Education | ☐ 32. Job Search | ☐ 54. Advertisement |
| ☑ 11. Gambling | ☐ 33. News and Media | ☐ 55. Web Hosting |
| ☐ 12. Alcohol/Tobacco | ☐ 34. Personals and Dating | ☐ 56. Other |
| ☑ 13. Chat/Instant Messaging (IM) | ☐ 35. Usenet News Groups | ☐ 57. Internet Watch Foundation CAIC |
| ☐ 14. Arts/Entertainment | ☐ 36. Reference | ☐ 58. Social Networking |
| ☐ 15. Business and Economy | ☐ 37. Religion | ☐ 59. Malware |
| ☐ 16. Abortion/Advocacy Groups | ☐ 38. Shopping | ☐ 60. N/A |
| ☐ 17. Education | ☐ 39. Internet Auctions | ☐ 61. N/A |
| ☐ 18. N/A | ☐ 40. Real Estate | ☐ 62. N/A |
| ☐ 19. Cultural Institutions | ☐ 41. Society and Lifestyle | ☐ 63. N/A |
| ☑ 20. Online Banking | ☐ 42. Gay and Lesbian Issues | ☐ 64. Not Rated |
| ☑ 21. Online Brokerage and Trading | ☐ 43. Restaurants and Dining | |
| ☐ 22. Games | ☐ 44. Sports/Recreation | |

**Students Filtering**

| | | |
|---|---|---|
| ☑ 1. Violence/Hate/Racism | ☐ 23. Government | ☐ 45. Travel |
| ☑ 2. Intimate Apparel/Swimsuit | ☐ 24. Military | ☐ 46. Vehicles |
| ☑ 3. Nudism | ☐ 25. Political/Advocacy Groups | ☐ 47. Humor/Jokes |
| ☑ 4. Pornography | ☐ 26. Health | ☑ 48. Multimedia |
| ☑ 5. Weapons | ☐ 27. Information Technology/Computers | ☑ 49. Freeware/Software Downloads |
| ☑ 6. Adult/Mature Content | ☑ 28. Hacking/Proxy Avoidance Systems | ☑ 50. Pay to Surf Sites |
| ☑ 7. Cult/Occult | ☐ 29. Search Engines and Portals | ☐ 51. N/A |
| ☑ 8. Drugs/Illegal Drugs | ☐ 30. E-Mail | ☐ 52. N/A |
| ☑ 9. Illegal Skills/Questionable Skills | ☑ 31. Web Communications | ☐ 53. Kid Friendly |
| ☐ 10. Sex Education | ☐ 32. Job Search | ☐ 54. Advertisement |
| ☑ 11. Gambling | ☐ 33. News and Media | ☐ 55. Web Hosting |
| ☑ 12. Alcohol/Tobacco | ☑ 34. Personals and Dating | ☐ 56. Other |
| ☑ 13. Chat/Instant Messaging (IM) | ☐ 35. Usenet News Groups | ☐ 57. Internet Watch Foundation CAIC |
| ☐ 14. Arts/Entertainment | ☐ 36. Reference | ☑ 58. Social Networking |
| ☐ 15. Business and Economy | ☐ 37. Religion | ☑ 59. Malware |
| ☐ 16. Abortion/Advocacy Groups | ☐ 38. Shopping | ☐ 60. N/A |
| ☐ 17. Education | ☐ 39. Internet Auctions | ☐ 61. N/A |
| ☐ 18. N/A | ☐ 40. Real Estate | ☐ 62. N/A |
| ☐ 19. Cultural Institutions | ☐ 41. Society and Lifestyle | ☐ 63. N/A |
| ☑ 20. Online Banking | ☐ 42. Gay and Lesbian Issues | ☑ 64. Not Rated |
| ☑ 21. Online Brokerage and Trading | ☐ 43. Restaurants and Dining | |
| ☑ 22. Games | ☐ 44. Sports/Recreation | |

# Mobile Technologies

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.
All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's Online Safety education program.

- **The school Acceptable Use Agreements for staff, pupils/students and parents/carers will give consideration to the use of mobile technologies**
- **The school allows:** (

| | School Devices | | | Personal Devices | | |
|---|---|---|---|---|---|---|
| | **School owned for single user** | **School owned for multiple users** | **Authorised device[1]** | **Student owned** | **Staff owned** | **Visitor owned** |

[1] Authorised device – purchased by the pupil/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

| | | | | | | |
|---|---|---|---|---|---|---|
| Allowed in school | *Yes* | *Yes* | *Yes* | *No* | *Yes/No* | *Yes/No* |
| Full network access | *Yes* | *Yes* | *Yes* | *no* | | |
| Internet only | | | | | | |
| No network access | | | | | | |

Aspects that the school may wish to consider and be included in their Online Safety Policy, Mobile Technologies Policy or Acceptable Use Agreements:

*School owned / provided devices:*

- *Who they will be allocated to*
- *Where, when and how their use is allowed – times / places / in school / out of school*
- *If personal use is allowed*
- *Levels of access to networks / internet (as above)*
- *Management of devices / installation of apps / changing of settings / monitoring*
- *Network / broadband capacity*
- *Technical support*
- *Filtering of devices*
- *Access to cloud services*
- *Data Protection*
- *Taking / storage / use of images*
- *Exit processes – what happens to devices / software / apps / stored data if user leaves the school*
- *Liability for damage*
- *Staff training*

Personal devices:

- Which users are allowed to use personal mobile devices in school (staff / pupils / students / visitors)
- Restrictions on where, when and how they may be used in school
- Storage
- Whether staff will be allowed to use personal devices for school business
- Levels of access to networks / internet (as above)
- Network / broadband capacity
- Technical support (this may be a clear statement that no technical support is available)
- Filtering of the internet connection to these devices
- Data Protection
- The right to take examine and search user's devices in the case of misuse (England only) – n.b. this must also be included in the Behaviour Policy.
- Taking / storage / use of images
- Liability for loss/damage or malfunction following access to the network (likely to be a disclaimer about school responsibility).
- Identification / labelling of personal devices
- How visitors will be informed about school requirements
- How education about the safe and responsible use of mobile devices is included in the school Online Safety education programmes.

# Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupil's 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:

- **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 e.g. on social networking sites.**
- **Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website / social media / local press** (see Parents / Carers Acceptable Use Agreement
- 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 / academy 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.
- 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.
- 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.

**At Assunnah Primary School we 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**

**Staff must ensure that they:**

- **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
- **the device must offer approved virus and malware checking software**
- **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**

Communications

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:

| | Staff & other adults | | | Students / Pupils | | | | |
|---|---|---|---|---|---|---|---|---|
| Communication Technologies | 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 the 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 e.g. tablets, gaming devices | | | | | | | | |
| Use of personal email addresses in school | | | | | | | | |
| Use of school email for personal emails | | | | | | | | |
| Use of messaging apps | | | | | | | | |
| Use of social media | | | | | | | | |
| Use of blogs | | | | | | | | |

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

- **The official *school* 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 email service to communicate with others when in school, or on school systems (e.g. by remote access).*
- **Users must immediately report, to the nominated person –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, social media, chat, blogs, VLE etc.) must be professional in tone and content.** *These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or 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 email addresses for educational use.*
- *Students / pupils should be taught about online 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 website and only official email addresses should be used to identify members of staff.*

# Social Media - Protecting Professional Identity

Assunnah Primary School provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: 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*
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official school social media accounts are established there should be:

- *A process for approval by senior leaders*
- *Clear processes for the administration and monitoring of these accounts – involving at least two members of staff*
- *A code of behaviour for users of the accounts, including*
- *Systems for reporting and dealing with abuse and misuse*
- *Understanding of how incidents may be dealt with under school disciplinary procedures*

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy

- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- *The school permits reasonable and appropriate access to private social media sites*

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process

The *school's* use of social media for professional purposes will be checked regularly by the senior risk officer Safeguarding officer (xxx) and to ensure compliance with the school policies

# Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. 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 / or outside the school when using school equipment or systems. The school policy restricts usage as follows:

| User Actions | | 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 | | | | | X |
| | Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003. | | | | | X |
| | Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008 | | | | | X |
| | 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 | | | | | X |
| | Pornography | | | | X | |
| | Promotion of any kind of discrimination | | | | X | |
| | threatening behaviour, including promotion of physical violence or mental harm | | | | X | |

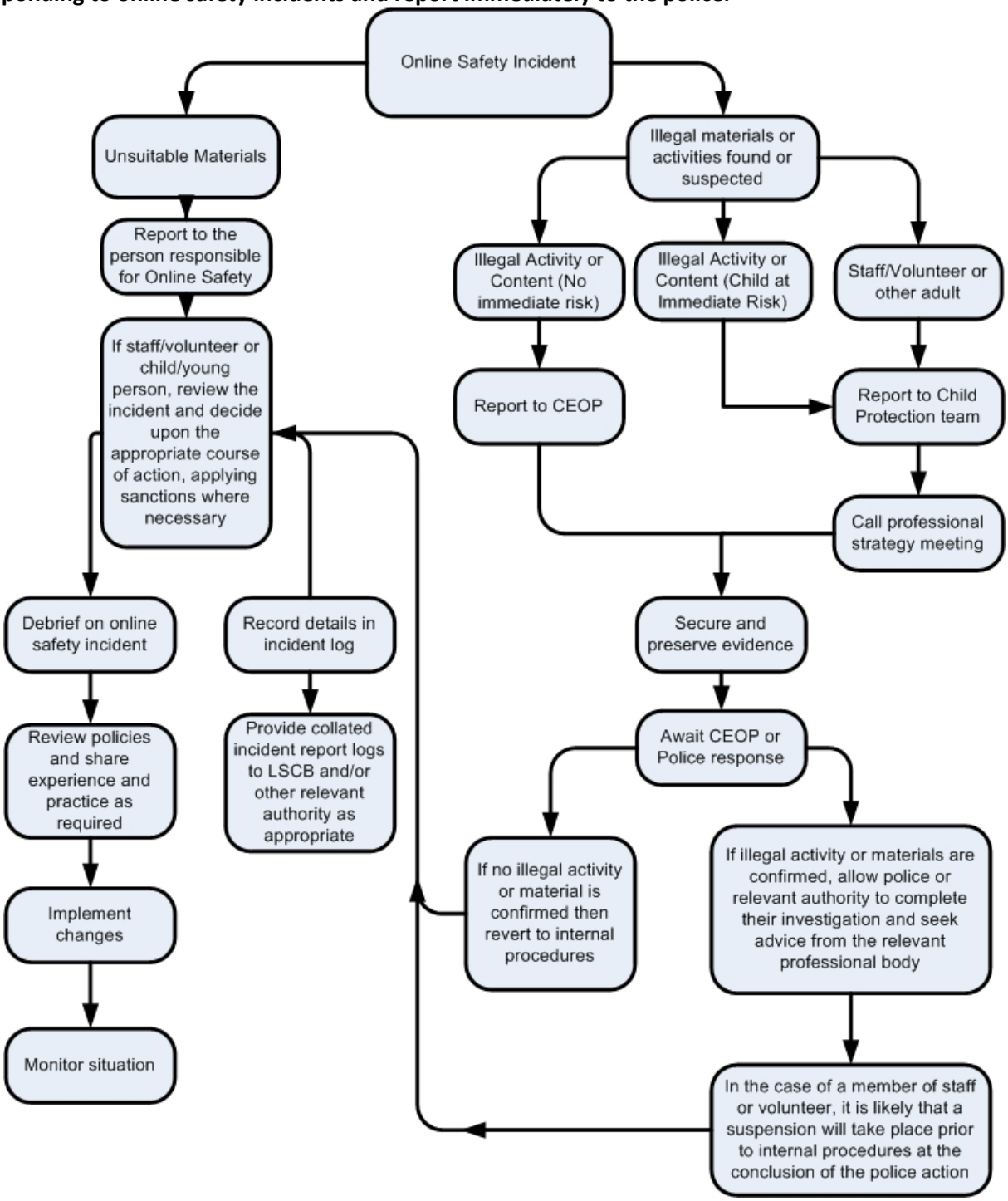
| | | | | | | |
|---|---|---|---|---|---|---|
| | Promotion of extremism or terrorism | | | | X | |
| | Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute | | | | X | |
| Using school systems to run a private business | | | | | X | |
| Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school | | | | | X | |
| Infringing copyright | | | | | X | |
| Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords) | | | | | X | |
| Creating or propagating computer viruses or other harmful files | | | | | X | |
| Unfair usage (downloading / uploading large files that hinders others in their use of the internet) | | | | | X | |
| On-line gaming (educational) | | | X | | | |
| On-line gaming (non-educational) | | | | | X | |
| On-line gambling | | | | | | X |
| On-line shopping / commerce | | | | | X | |
| File sharing | | | | X | | |
| Use of social media | | | | X | | |
| Use of messaging apps | | | | X | | |
| Use of video broadcasting e.g. YouTube | | | | X | | |

# Responding to incidents of misuse

This guidance is intended for use when staffs 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). In all situations staff will need to report to the designated safeguarding officer (Mrs Xxx Ali).

# 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.**



# Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school. 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 Group 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
    - promotion of terrorism or extremism
    - 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* and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

# Actions & Sanctions

The school will deal with incidents that involve inappropriate rather than illegal misuse very seriously. 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:

| | Actions / Sanctions | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Students / Pupils Incidents | Refer to class teacher / tutor | Refer to Head of Department / Year / other | Refer to Headteacher / | Refer to Police | Refer to technical support staff for action re filtering / security etc. | Inform parents / carers | Removal of network / internet access rights | Warning | Further sanction eg detention / exclusion |
| Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities). | | X | X | X | | | | | |
| Unauthorised use of non-educational sites during lessons | | | | | | | | | |
| Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device | | | | | | | | | |
| Unauthorised / inappropriate use of social media / messaging apps / personal email | | | | | | | | | |
| Unauthorised downloading or uploading of files | | | | | | | | | |
| Allowing others to access school network by sharing username and passwords | | | | | | | | | |
| Attempting to access or accessing the school 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 | | | | | | | | | |

**Actions / Sanctions**

| Staff Incidents | Refer to line manager | Refer to Headteacher | Refer to Local Authority / HR | Refer to Police | Refer to Technical Support Staff for action re filtering etc. | Warning | Suspension | Disciplinary action |
|---|---|---|---|---|---|---|---|---|
| **Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).** | | X | X | X | | | | |
| Inappropriate personal use of the internet / social media / personal email | | | | | | | | |
| Unauthorised downloading or uploading of files | | | | | | | | |
| Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account | | | | | | | | |
| Careless use of personal data e.g. holding or transferring data in an insecure manner | | | | | | | | |
| Deliberate actions to breach data protection or network security rules | | | | | | | | |
| Corrupting or destroying the data of other users or causing deliberate damage to hardware or software | | | | | | | | |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | | | | | | | | |
| Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils | | | | | | | | |
| Actions which could compromise the staff member's professional standing | | | | | | | | |
| Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school | | | | | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 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 | | | | | | | | |
| Breaching copyright or licensing regulations | | | | | | | | |
| Continued infringements of the above, following previous warnings or sanctions | | | | | | | | |

# Student / Pupil Acceptable Use Agreement Form

This form relates to the *student / pupil* Acceptable Use Agreement, to which it is attached.
Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems.
I have read and understand the above and agree to follow these guidelines when:

- I use the *school* systems and devices (both in and out of school)
- I use my own devices in the *school* (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I use my own equipment out of the school in a way that is related to me being a member of this *school* e.g. communicating with other members of the school, accessing school email, VLE, website etc.

Name of Student / Pupil: .....
Group / Class: .....
Signed: .....
Date: .....

# Student / Pupil Acceptable Use Policy Agreement Template – for younger pupils (Foundation / KS1)

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers / tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable 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 / tablet

Signed (child): .....

Signed (parent): .....

# Parent / Carer Acceptable Use Agreement Template

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that *students / pupils* will have good access to digital technologies to enhance their learning and will, in return, expect the *students / pupils* to agree to be responsible users. A copy of the Student / Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

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

Parent / Carer Permission Form

Parent / Carers Name: .....

Student / Pupil Name: .....

As the parent / carer of the above *students / pupils*, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

Either: (KS2 and above)

*I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.*

Or: (KS1)

*I understand that the school has discussed the Acceptable Use Agreement with my son / daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of 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 systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

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

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 online safety.

Signed: .....

Date: .....

# Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Students / Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.
Images may also be used to celebrate success through their publication in newsletters, on the 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. We will also ensure that when images are published that the young people cannot be identified by the use of their names.
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.
Parents / carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents / carers to agree

### Digital / Video Images Permission Form

Parent / Carers Name: .....
Student / Pupil Name: .....

| | |
|---|---|
| As the parent / carer of the above student / pupil, I agree to the school taking and using digital / video images of my child / children. 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. | Yes / No |
| I agree that if I take digital or video images at, or of – school events which include images of children, other than my own, I will abide by these guidelines in my use of these images. | Yes / No |

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

# Student / Pupil Acceptable Use Agreement

On the following pages we have copied, for the information of parents and carers, the Student / Pupil Acceptable Use Agreement.

# Staff (and Volunteer) Acceptable Use Policy Agreement Template

## School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools / academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These

technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school / academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for *students / pupils* learning and will, in return, expect staff and volunteers to agree to be responsible users.

# Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the *school* will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology 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 by the school. (schools should amend this section in the light of their policies which relate to the personal use, by staff and volunteers, of school systems)
- 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 understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, 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 / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner

- I will not engage in any on-line activity that may compromise my professional responsibilities.

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

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using *school / academy* equipment. I will also follow any additional rules set by the *school* about such use. 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 unless permission granted..
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (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.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School/ LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student / 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 / academy policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school 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 the *school*:

- I understand that this Acceptable Use Policy applies not only to my work and use of school / academy digital technology equipment in school, but also applies to my use of school / academy systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include suspension or loss of job. a warning, a suspension, referral to Proprietor / Directors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name: .....

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

# Acceptable Use Agreement for Community Users Template

This Acceptable Use Agreement is intended to ensure:

- that community users of school / academy digital technologies will be responsible users and stay safe while using these systems and devices
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential risk in their use of these systems and devices

## Acceptable Use Agreement

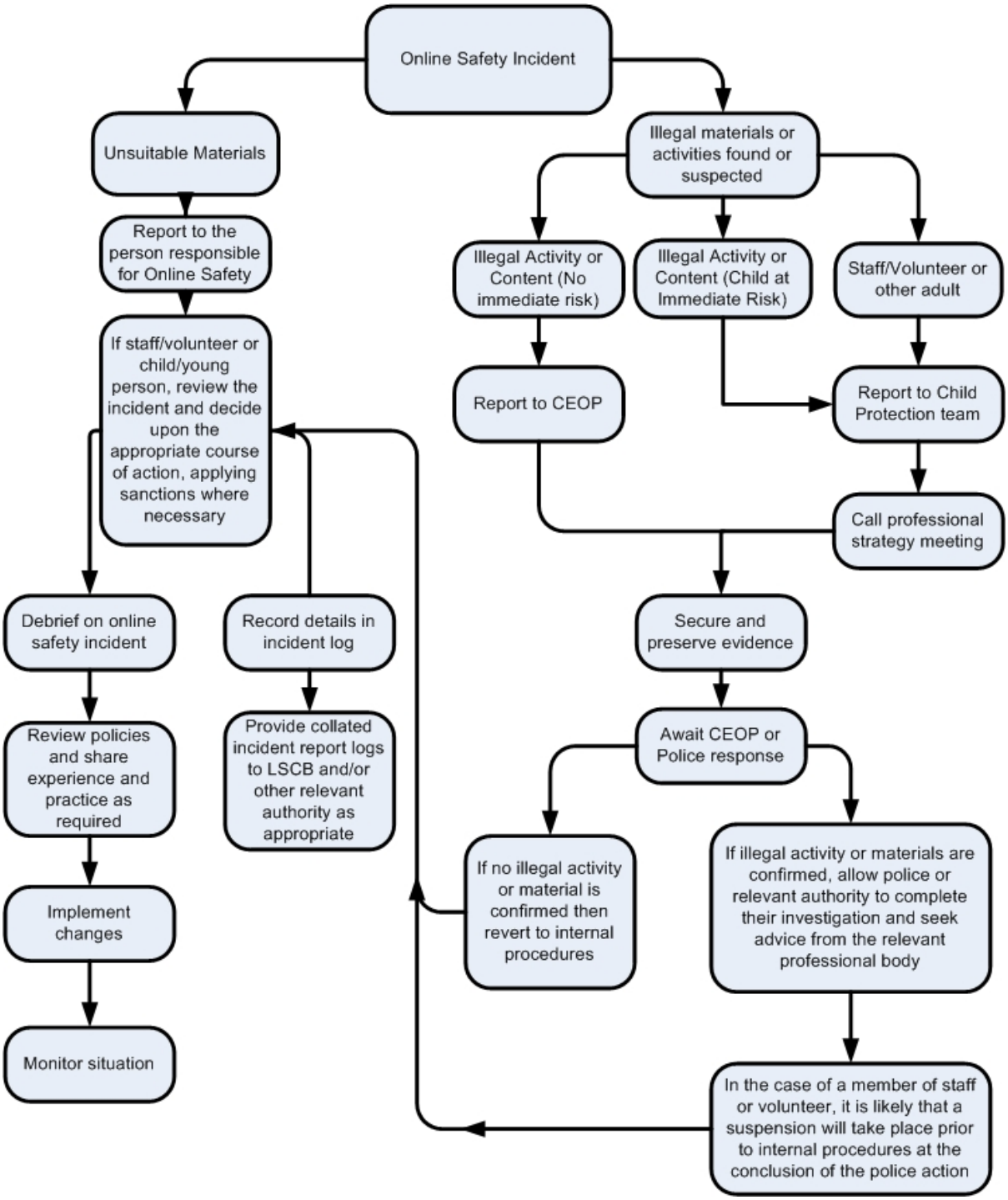
I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school:

- I understand that my use of school / academy) systems and devices and digital communications will be monitored
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist 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 immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and / or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, 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 school device, nor will I try to alter computer settings, unless I have permission to do so.
- 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 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 if I fail to comply with this Acceptable Use Agreement, the school has the right to remove my access to school systems / devices

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

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

# Responding to incidents of misuse – flow chart




# 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

| | |
|---|---|
| | |
| | |
| | |
| | |
| | |

# Reporting Log

Group: .....

| Date | Time | Incident | Action Taken | | Incident Reported By | Signature |
|---|---|---|---|---|---|---|
| | | | What? | By Whom? | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

# Training Needs Audit Log

Group: .....

| Relevant training the last 12 months | Identified Training Need | To be met by | Cost | Review Date |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |

ONLINE SAFETY MONITORING

| | | | | |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# School Technical Security Policy Template (including filtering and passwords)

### Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the *school infrastructure / network* is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems
- there is oversight from senior leaders, and these have impact on policy and practice.

## Responsibilities

The management of technical security will be the responsibility of Feroz Adam

## Technical Security

### Policy statements

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 receive guidance and training and will be effective in carrying out their responsibilities:

- **School technical systems will be managed in ways that ensure that the school meets recommended technical requirements**
- **There will be regular reviews and audits of the safety and security of school technical systems**
- **Servers, wireless systems and cabling must be securely located and physical access restricted**
- **Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, workstations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.**
- **Office door is kept locked when not in use and supervised by a designated staff when open.**
- **Responsibilities for the management of technical security are clearly assigned to appropriate and well-trained staff** Feroz Adam
- **All users will have clearly defined access rights to school technical systems.** *Details of the access rights available to groups of users will be recorded by the Network Manager Feroz Adam and will be reviewed, at least annually by Senior leadership team).*
- Users will be made responsible for the security of their username and password must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security Feroz Adam 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

- *Mobile device security and management procedures are in place.* The school mobiles that are allowed on site is 07429112217 the mobile device security procedures that are in use).
- School technical staff regularly monitors and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement. (*Remote management tools are used by staff to control workstations and view users activity*
- An agreed decision will be made for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school system.
- *An agreed policy is in place regarding the downloading of executable files and the installation of programmes on school devices by users*
- *An agreed policy is in place 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 regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices*
- *The school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc*
- *Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.*

# Password Security

A safe and secure username / password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and Virtual Learning Environment (VLE).

## Policy Statements

- All users will have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the Online Safety Group (or other group).
- **All school networks and systems will be protected by secure passwords that are regularly changed**
- **The "master / administrator" passwords for the school systems, used by the technical staff must also be available to the *Headteacher /* or other nominated senior leader and kept in a secure place e.g. school safe. Consideration should also be given to using two factor authentication for such accounts.**
- 
- All users (adults and young people) will have responsibility for the security of their username and password must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- *Passwords for new users, and replacement passwords for existing users will be allocated by Feroz Adam*
- *Any changes carried out must be notified to the manager of the password security policy (above). Or:*
- *Passwords for new users and replacement passwords for existing users will be issued through an automated process* via the MS 365 admin portal
- *Users will change their passwords at regular intervals – as described in the staff and student / pupil sections below* (The level of security required may vary for staff and student / pupil accounts and the sensitive nature of any data accessed through that account)
- *Where passwords are set / changed manually requests for password changes should be authenticated by (the responsible person) to ensure that the new password can only be passed to the genuine user* (the school will need to decide how this can be managed – possibly by requests being authorised by

a line manager for a request by a member of staff or by a member of staff for a request by a pupil / student)

### Staff Passwords

- **All staff users will be provided with a username and password** by (insert name or title / automated process) who / which will keep an up-to-date record of users and their usernames.
- the password should be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special characters
- *must not include proper names or any other personal information about the user that might be known by others*
- *the account should be "locked out" following six successive incorrect log-on attempts*
- *temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on*
- *passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption)*
- *passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school*
- should be changed at least every 60 to 90 days
- should not re-used for 6 months and be significantly different from previous passwords created by the same user*. The last four passwords cannot be re-used*.
- **When required users** (at KS2 and above) **will be provided with a username and password** by Feroz Adam who / which will keep an up-to-date record of users and their usernames.
- *Users will be required to change their password every 4 week*
- Students / pupils will be taught the importance of password security

### Training / Awareness

It is essential that users should be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access / data loss. This should apply to even the youngest of users, even if class log-ins are being used.

Members of staff will be made aware of the school's password policy:

- at induction
- through the school's online safety policy and password security policy
- through the Acceptable Use Agreement

Pupils / students will be made aware of the school's password policy:

- in lessons
- through the Acceptable Use Agreement

### Audit / Monitoring / Reporting / Review

The responsible person (insert title) will ensure that full records (manual or automated) are kept of:

- User Ids and requests for password changes
- *User log-ins*
- *Security incidents related to this policy*

## Filtering

### Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in

a larger strategy for online safety and acceptable use. It is 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.

## Responsibilities

The responsibility for the management of the school's filtering policy will be held by them will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.
To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must

- **be logged in change control logs**

All users have a responsibility to report immediately to (insert title) any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.
Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

## Policy Statements

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content list . Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

- *Either – we will supports the managed filtering service provided by the Internet Service Provider* (or other filtering service provider)
- *Or – The school manages its own filtering service* (n.b. If we decides to remove the external filtering and replace it with another internal filtering system, this will be clearly explained in the policy and evidence provided that the Headteacher / would be able to show, in the event of any legal issue that the school was able to meet its statutory requirements to ensure the safety of staff / students / pupils)
- *The school has provided enhanced / differentiated user-level filtering through the use of the* (insert name) *filtering programme. (allowing different filtering levels for different ages / stages and different groups of users – staff / pupils / students etc.)*
- *In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher / (or other nominated senior leader).*
- *Mobile devices that access the school / academy internet connection (whether school / academy or personal devices) will be subject to the same filtering standards as other devices on the school systems*
- *Any filtering issues should be reported immediately to the filtering provider.*
- *Requests from staff for sites to be removed from the filtered list will be considered by the technical staff* (Feroz Adam) *If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the team.*

## Education / Training / Awareness

*Pupils / students* will be made aware of the importance of filtering systems through the online safety education programme (schools may wish to add details). They will also be warned of the consequences of attempting to subvert the filtering system.
Staff users will be made aware of the filtering systems through: (amend as relevant)

- the Acceptable Use Agreement
- induction training
- staff meetings, briefings, Inset.

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

### Changes to the Filtering System

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to (Feroz Adam) who will decide whether to make school level changes (as above).

Staff can email the DSL and request the appropriate changes to filtering. This will then be reviewed and adapted accordingly. The following will be considered prior to making changes:

- the grounds on which changes may be allowed or denied (we may choose to allow access to some sites e.g. social networking sites for some users, at some times, or for a limited period of time. There should be strong educational reasons for changes that are agreed).
- how a second responsible person will be involved to provide checks and balances (preferably this will be at the time of request, but could be retrospectively through inspection of records / audit of logs) any audit / reporting system

## Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School Online Safety Policy and the Acceptable Use Agreement. *Monitoring will take place as follows*

### Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to: (Headteacher, DSL, IT manager)

- the second responsible person (Business Manager)
- Online Safety Group
- Online Safety Governor / Governors committee
- External Filtering provider / Local Authority / Police on request

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision. (The evidence might show a large number of requests to remove the filtering from sites – in which case schools might question whether their current level of filtering is too restrictive for educational purposes. Alternatively, a large number of incidents where users try to subvert the filtering system might suggest that improved monitoring / disciplinary action might be necessary).

***Imperro is used as an additional filtering service and-it will give us alerts.**
**Microsoft Internet safety as part of the Office 365 for Education suite is also being used**

### Further Guidance

The following is recommended:

*"to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering"* (Revised Prevent Duty Guidance: for England and Wales, April 2021).

Furthermore the Department for Education published proposed changes to 'Keeping Children Safe in Education' September 2023. Amongst the proposed changes, schools will be obligated to *"ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access*

*harmful or inappropriate material from the school or colleges IT system"* however, schools will need to *"be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."*
In response UKSIC produced guidance on – information on "Appropriate Filtering"
NEN Technical guidance: http://www.nen.gov.uk/e-security-managing-and-maintaining-e-securitycyber-security-in-schools/
Somerset Guidance for schools – this checklist is particularly useful where a school / academy uses external providers for its technical support / security: https://360safe.org.uk/Files/Documents/Somerset-Questions-for-Technical-Support-v4.aspx

# School Personal Data Handling Policy Template

## School Personal Data Handling Policy

### Introduction

At Assunnah Primary School all employees should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature
It is the responsibility of all members of the school community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:

- have permission to access that data, and/or
- need to have access to that data.

Data breaches can have serious effects on individuals and / or institutions concerned, can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office - for the school and the individuals involved. Particularly, all transfer of data is subject to risk of loss or contamination.
Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data protection legislation and relevant regulations and guidance (where relevant from the Local Authority).

### Policy Statements

The school 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 below)

### Personal Data

The school and individuals will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the school community – including *pupils / students*, members of staff and parents / carers e.g. names, addresses, contact details, legal guardianship contact details, health records, disciplinary records
- Curricular / academic data e.g. class lists, pupil / student progress records, reports, references
- Professional records e.g. employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members.

### Responsibilities

The school's safeguarding officers Hodan Yusuf, Xxx, Mohammed Yusuf will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the school's information risk policy and risk assessment

The school will identify Information Asset Owners (IAOs) Feroz Adam *for the various types of* data being held (e.g. pupil / student information / staff information / assessment data etc.). The IAOs will manage and address risks to the information and will understand:

- what information is held, for how long and for what purpose,

- how information as been amended or added to over time, and
- who has access to protected data and why.

Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.
Proprietors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Proprietor.

## Registration

The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner. (each school is responsible for their own registration):
http://www.ico.gov.uk/what_we_cover/register_of_data_controllers.aspx

## Information to Parents / Carers – the "Privacy Notice"

In order to comply with the fair processing requirements of the DPA, the school will inform parents / carers of all pupils / students of the data they collect, process and hold on the pupils / students, the purposes for which the data is held and the third parties (e.g. LA, DfE, etc) to whom it may be passed. This privacy notice will be passed to parents / carers through Prospectus, newsletters, reports or a specific letter / communication). Parents / carers of young people who are new to the school will be provided with the privacy notice through them.
More information about the suggested wording of privacy notices can be found on the DfE website:

## Training & awareness

All staff will receive data handling awareness / data protection training and will be made aware of their responsibilities, as described in this policy through: Induction training for new staff

- Staff meetings / briefings / Inset
- Day to day support and guidance from Information Asset Owners
- Risk Assessments

Information risk assessments will be carried out by Information Asset Owners to establish the security measures already in place and whether they are the most appropriate and cost effective. The risk assessment will involve:

- Recognising the risks that are present;
- Judging the level of the risks (both the likelihood and consequences); and
- Prioritising the risks.

Risk assessments are an ongoing process and should result in the completion of an Information Risk Actions Form (example below):

| Risk ID | Information Asset affected | Information Asset Owner | Protective Marking (Impact Level) | Likelihood | Overall risk level (low, medium, high) | Action(s) to minimise risk |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |

## Impact Levels and protective marking

Following incidents involving loss of data, the Government recommends that the Protective Marking Scheme should be used to indicate the sensitivity of data. The Protective Marking Scheme is mapped to Impact Levels as follows:

| Government Protective Marking Scheme label | Impact Level (IL) | Applies to schools? |
|---|---|---|
| **Not Protectively Marked** | 0 | Will apply in schools |
| **Protect** | 1 or 2 | |
| **Restricted** | 3 | |
| **Confidential** | 4 | Will not apply in schools |
| **Highly Confidential** | 5 | |
| **Top Secret** | 6 | |

Most student / pupil or staff personal data that is used within educational institutions will come under the PROTECT classification. However, some, e.g. the home address of a child (or vulnerable adult) at risk will be marked as RESTRICT.
The school will ensure that all school staff, independent contractors working for it, and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as Protect, Restricted or higher. Unmarked material is considered 'unclassified'. The term 'UNCLASSIFIED' or 'NON' or 'NOT PROTECTIVELY MARKED' may be used to indicate positively that a protective marking is not needed.
All documents (manual or digital) that contain protected or restricted data will be labelled clearly with the Impact Level shown in the header and the Release and Destruction classification in the footer.
Users must be aware that when data is aggregated the subsequent impact level may be higher than the individual impact levels of the original data. Combining more and more individual data elements together in a report or data view increases the impact of a breach. A breach that puts students / pupils at serious risk of harm will have a higher impact than a risk that puts them at low risk of harm. Long-term significant damage to anyone's reputation has a higher impact than damage that might cause short-term embarrassment.
Release and destruction markings should be shown in the footer e.g. "Securely delete or shred this information when you have finished using it".

## Secure Storage of and access to data

The school will ensure that systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.
All users will use strong passwords which must be changed regularly (insert relevant school details as per the school's password security policy). User passwords must never be shared.
Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.
All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.
Personal data can only be stored on school equipment (this includes computers and portable storage media (where allowed). Private equipment (i.e. owned by the users) must not be used for the storage of personal data.
When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected,
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected),
- the device must offer approved virus and malware checking software (memory sticks will not provide this facility, most mobile devices will not offer malware protection), and
- 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* has clear policy and procedures for the use of "Cloud Based Storage Systems" on Microsoft 365, google apps and google docs) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data.
(see appendix for further information and the ICO Guidance:
http://www.ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Practical_application/cloud_computing_guidance_for_organisations.ashx
As a Data Controller, the *school* is responsible for the security of any data passed to a "third party". Data Protection clauses will be included in all contracts where data is likely to be passed to a third party.
All paper based Protected and Restricted (or higher) material must be held in lockable storage, whether on or off site.
The *school / academy* recognises that under Section 7 of the DPA,
http://www.legislation.gov.uk/ukpga/1998/29/section/7 data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place (insert details here) to deal with Subject Access Requests i.e. a written request to see all or a part of the personal data held by the data controller in connection with the data subject. Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

## Secure transfer of data and access out of school

The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location (see earlier section – LA / Academy Group / school policies may forbid such transfer);
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform;
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location;
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software; and
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority (if relevant) in this event.

## Disposal of data

The school will comply with the requirements for the safe destruction of personal data when it is no longer required.
The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance (see earlier section for reference to the Cabinet Office guidance), and other media must be shredded, incinerated or otherwise disintegrated for data.
*A Destruction Log should be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.*

## Audit Logging / Reporting / Incident Handling

It is good practice, as recommended in the "Data Handling Procedures in Government" document that the activities of data users, in respect of electronically held personal data, will be logged and these logs will be monitored by responsible individuals. (Xxx)
The audit logs will be kept to provide evidence of accidental or deliberate data security breaches – including loss of protected data or breaches of an acceptable use policy, for example.
The school has a policy for reporting, managing and recovering from information risk incidents, which establishes: (

- a "responsible person" for each incident;
- a communications plan, including escalation procedures;
- and results in a plan of action for rapid resolution; and
- a plan of action of non-recurrence and further awareness raising.

All significant data protection incidents must be reported through the SIRO to the Information Commissioner's Office based upon the local incident handling policy and communication plan.

## Use of technologies and Protective Marking

The following provides a useful guide:

| | The information | The technology | Notes on Protect Markings (Impact Level) |
|---|---|---|---|
| **School life and events** | School terms, holidays, training days, the curriculum, extra-curricular activities, events, displays of pupils work, lunchtime menus, extended services, parent consultation events | Common practice is to use publically accessible technology such as school websites or portal, emailed newsletters, subscription text services | Most of this information will fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category. |
| **Learning and achievement** | Individual pupil / student academic, social and behavioural achievements, progress with learning, learning behaviour, how parents can support their child's learning, assessments, attainment, attendance, individual and personalised curriculum and educational needs. | Typically schools will make information available by parents logging on to a system that provides them with appropriately secure access, such as a Learning Platform or portal, or by communication to a personal device or email account belonging to the parent. | Most of this information will fall into the PROTECT (Impact Level 2) category. There may be students/ pupils whose personal data requires a RESTRICTED marking (Impact Level 3) or higher. For example, the home address of a child at risk. In this case, the school may decide not to make this pupil / student record available in this way. |

| | | | |
|---|---|---|---|
| **Messages and alerts** | Attendance, behavioural, achievement, sickness, school closure, transport arrangements, and other information that it may be important to inform or contact a parent about as soon as possible. This may be particularly important when it is necessary to contact a parent concerning information that may be considered too sensitive to make available using other online means. | Email and text messaging are commonly used by schools to contact and keep parents informed. Where parents are frequently accessing information online then systems e.g. Learning Platforms or portals, might be used to alert parents to issues via "dashboards" of information, or be used to provide further detail and context. | Most of this information will fall into the PROTECT (Impact Level 1) category. However, since it is not practical to encrypt email or text messages to parents, schools should not send detailed personally identifiable information. General, anonymous alerts about schools closures or transport arrangements would fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category. |

ASSUNNAH PRIMARY SCHOOL PRIVACY NOTICE

for

*Pupils in Schools,*

## Privacy Notice - Data Protection Act 1998

We **Assunnah Primary School** are a data controller for the purposes of the Data Protection Act. We collect information from you and may receive information about you from your previous school and the Learning Records Service. We hold this personal data and use it to:

- Support your teaching and learning;
- Monitor and report on your progress;
- Provide appropriate pastoral care, and
- Assess how well your school is doing.

This information includes your contact details, national curriculum assessment results, attendance information and personal characteristics such as your ethnic group, any special educational needs and relevant medical information. If you are enrolling for post 14 qualifications we will be provided with your unique learner number (ULN) by the Learning Records Service and may also obtain from them details of any learning or qualifications you have undertaken.

***We will not give information about you to anyone outside the school without your consent unless the law and our rules allow us to.***

We are required by law to pass some information about you to the Local Authority and the Department for Education (DfE)

If you want to see a copy of the information about you that we hold and/or share, please contact (**Mis xxx.**

If you require more information about how the Local Authority (LA) and/or DfE store and use your information, then please go to the following websites:
https://new.haringey.gov.uk/council-elections/data-finance/information-data-requests/data-protection-privacy/privacy-statements
and
http://www.education.gov.uk/researchandstatistics/datatdatam/b00212337/datause
If you are unable to access these websites we can send you a copy of this information. Please contact the LA or DfE as follows:

Haringey Customer Service Centres

Marcus Garvey Centre - Library and Customer Services - N15 4JA
Wood Green Library and Customer Services - N22 6XD

Opening times

Monday Tuesday, Thursday and Friday, 9am to 5pm
Wednesday, 10am to 5pm

| | |
|---|---|
| Website: | www.education.gov.uk |
| Email: | http://www.education.gov.uk/help/contactus |
| Telephone: | 0370 000 2288 |

# Electronic Devices - Searching & Deletion policy

## Introduction

The changing face of information technologies and ever-increasing pupil / student use of these technologies has meant that the Education Acts have had to change in an attempt to keep pace. Within Part 2 of the Education Act 2011 (Discipline) there have been changes to the powers afforded to schools by statute to search pupils in order to maintain discipline and ensure safety. Schools are required to ensure they have updated policies which take these changes into account. No such policy can on its own guarantee that the school will not face legal challenge, but having a robust policy which takes account of the Act and applying it in practice will however help to provide the school with justification for what it does.
The particular changes we deal with here are the added power to search for items 'banned under the school rules' and the power to 'delete data' stored on seized electronic devices.
Items banned under the school rules are determined and publicised by the Headteacher (section 89 Education and Inspections Act 1996).
An item banned by the school rules may only be searched for under these new powers if it has been identified in the school rules as an item that can be searched for. It is therefore important that there is a school policy which sets out clearly and unambiguously the items which:

- are banned under the school rules; and
- are banned AND can be searched for by authorised school staff

The act allows authorised persons to examine data on electronic devices if they think there is a good reason to do so. In determining a 'good reason' to examine or erase the data or files the authorised staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or could break the school rules.
Following an examination, if the person has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.
The *Head Teacher /* must publicise the school behaviour policy, in writing, to staff, parents / carers and students / pupils at least once a year. (There should therefore be clear links between the search etc. policy and the behaviour policy).
DfE advice on these sections of the Education Act 2011 can be found in the document: "Screening, searching and confiscation – Advice for head teachers, staff and governing bodies"
http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation
It is recommended that Headteachers / s (and, at the least, other senior leaders) should be familiar with this guidance.

## Relevant legislation:

- Education Act 1996
- Education and Inspections Act 2006
- Education Act 2011 Part 2 (Discipline)
- The School Behaviour (Determination and Publicising of Measures in Academies) Regulations 2012
- Health and Safety at Work etc. Act 1974
- Obscene Publications Act 1959
- Children Act 1989
- Human Rights Act 1998
- Computer Misuse Act 1990

## Responsibilities

The *Headteacher* is responsible for ensuring that the school policies reflect the requirements contained within the relevant legislation. The formulation of these policies may be delegated to other individuals or groups. The policies will normally be taken to Proprietor/s for approval. The Headteacher will need to authorise those staff who are allowed to carry out searches.
This policy has been written by and will be reviewed by: xxx
The *Headteacher /* has authorised the following members of staff to carry out searches for and of electronic devices and the deletion of data / files on those devices: xxx
The *Headteacher /* may authorise other staff members in writing in advance of any search they may undertake, subject to appropriate training.

## Training / Awareness

Members of staff should be made aware of the school's policy on "Electronic devices – searching and deletion":

- at induction
- at regular updating sessions on the school's online safety policy

Members of staff authorised by the Headteacher / to carry out searches for and of electronic devices and to access and delete data / files from those devices should receive training that is specific and relevant to this role.
Specific training is required for those staff who may need to judge whether material that is accessed is inappropriate or illegal.

# Policy Statements

## Search:

The school Behaviour Policy refers to the policy regarding searches with and without consent for the wide range of items covered within the Education Act 2011 and lists those items. This policy refers only to the searching for and of electronic devices and the deletion of data / files on those devices.
**Either:**
*Pupils/students are not allowed to bring mobile phones or other personal electronic devices to school or use them in the school.*
**Or**
*Pupils / students are allowed to bring mobile phones or other personal electronic devices to school and use them only within the rules laid down by the school.* (you should refer to the relevant policy or to list here the conditions under which they are allowed)
If pupils / students breach these roles:
**Either:**
*The sanctions for breaking these rules will be:* (list here)
**Or**
*The sanctions for breaking these rules can be found in the* (name the policy - for many schools this will be the Behaviour Policy)
Authorised staff (defined in the responsibilities section above) have the right to search for such electronic devices where they reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules.

- Searching with consent - Authorised staff may search with the pupil's consent for any item

- Searching without consent - Authorised staff may only search without the pupil's consent for anything which is either 'prohibited' (as defined in Section 550AA of the Education Act 1996) or appears in the school rules as an item which is banned and may be searched for

**In carrying out the search:**

The authorised member of staff must have reasonable grounds for suspecting that a *student / pupil* is in possession of a prohibited item i.e. an item banned by the school rules and which can be searched for. (Whether there are 'reasonable grounds' is a matter decided on by reference to the circumstances witnessed by, or reported to, someone who is authorised and who exercises properly informed professional judgment and has received appropriate training).

The authorised member of staff should take reasonable steps to check the ownership of the mobile phone / personal electronic device before carrying out a search. (The powers included in the Education Act do not extend to devices owned (or mislaid) by other parties e.g. a visiting parent or contractor, only to devices in the possession of pupils / students.)

The authorised member of staff should take care that, where possible, searches should not take place in public places e.g. an occupied classroom, which might be considered as exploiting the student / pupil being searched.

The authorised member of staff carrying out the search must be the same gender as the *student / pupil* being searched; and there must be a witness (also a staff member) and, if at all possible, they too should be the same gender as the *student/ pupil* being searched.

There is a limited exception to this rule: Authorised staff can carry out a search of a *student / pupil* of the opposite gender including without a witness present, but **only where you reasonably believe that there is a risk that serious harm will be caused to a person if you do not conduct the search immediately and where it is not reasonably practicable to summon another member of staff.**

**Extent of the search:**

**The person conducting the search may not require the *student/ pupil* to remove any clothing other than outer clothing.**

Outer clothing means clothing that is not worn next to the skin or immediately over a garment that is being worn as underwear (outer clothing includes hats; shoes; boots; coat; blazer; jacket; gloves and scarves).

'Possessions' means any goods over which the *student / pupil* has or appears to have control – this includes desks, lockers and bags. (schools will need to take account of their normal policies regarding religious garments / headwear and may wish to refer to it in this policy)

*A student's / pupil's* possessions can only be searched in the presence of the *student / pupil* and another member of staff, except where there is a risk that serious harm will be caused to a person if the search is not conducted immediately and where it is not reasonably practicable to summon another member of staff.

**The power to search without consent enables a personal search, involving removal of outer clothing and searching of pockets; but not an intimate search going further than that, which only a person with more extensive powers (e.g. a police officer) can do.**

**Use of Force – force cannot be used to search without consent for items banned under the school rules regardless of whether the rules say an item can be searched for.**

# Electronic devices

An authorised member of staff finding an electronic device may access and examine any data or files on the device if they think there is a good reason to do so (i.e. the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules).

The examination of the data / files on the device should go only as far as is reasonably necessary to establish the facts of the incident. Any further intrusive examination of personal data may leave the school open to legal challenge. It is important that authorised staff should have training and sufficient knowledge of electronic devices and data storage.

**If inappropriate material is found on the device it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police. Examples of illegal activity would include:**

- child sexual abuse images (including images of one child held by another child)
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

Members of staff may require support in judging whether the material is inappropriate or illegal. One or more Senior Leaders should receive additional training to assist with these decisions. Care should be taken not to delete material that might be required in a potential criminal investigation.
The school should also consider their duty of care responsibility in relation to those staff who may access disturbing images or other inappropriate material whilst undertaking a search. Seeing such material can be most upsetting. There should be arrangements in place to support such staff. The school may wish to add further detail about these arrangements.
Further guidance on reporting the incident to the police and the preservation of evidence can be found in the SWGfL flow chart in the main School Template Policies document. Local authorities / LSCBs may also have further guidance, specific to their area.

# Deletion of Data

Following an examination of an electronic device, if the authorised member of staff has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so. (i.e. the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules).
If inappropriate material is found on the device, it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a possible criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police. (It is recommended that members of staff should know who to contact, within school, for further guidance before taking action and that the person or persons is or are named within this policy).
*A record should be kept of the reasons for the deletion of data / files.* (DfE guidance states and other legal advice recommends that there is no legal reason to do this, best practice suggests that the school can refer to relevant documentation created at the time of any search or data deletion in the event of a pupil /student, parental or other interested party complaint or legal challenge. Records will also help the school to review online safety incidents, learn from what has happened and adapt and report on application of policies as necessary).

# Care of Confiscated Devices

School staff are reminded of the need to ensure the safe keeping of confiscated devices, to avoid the risk of compensation claims for damage / loss of such devices (particularly given the possible high value of some of these devices).
The school may wish to add a disclaimer to the relevant section of the Behaviour Policy which may assist in covering the school against damage / loss claims.

# Audit / Monitoring / Reporting / Review

The responsible person (Xxx) will ensure that full records are kept of incidents involving the searching for and of mobile phones and electronic devices and the deletion of data / files. (a template log sheet can be found in the appendices to the School Online Safety Template Policies)

These records will be reviewed by ... (Online Safety Officer / Online Safety Committee / Online Safety Governor) at regular intervals (state the frequency).

This policy will be reviewed by the head teacher and proprietor annually and in response to changes in guidance and evidence gained from the records.

The school is required is publish its Behaviour Policy to parents annually (including on its website) – the Behaviour Policy should be cross referenced with this policy on search and deletion.

DfE guidance can be found at: https://www.gov.uk/government/publications/searching-screening-and-confiscation

Mobile Technologies Template Policy (Inc. BYOD/BYOT)Mobile technology devices may be a school owned/provided or privately owned smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.
The absolute key to considering the use of mobile technologies is that the pupils / students, staff and wider school community understand that the primary purpose of having their personal device at school is educational and that this is irrespective of whether the device is school owned/provided or personally owned. The mobile technologies policy should sit alongside a range of polices including but not limited to the Safeguarding Policy, Bullying Policy, Acceptable Use Policy, policies around theft or malicious damage and the Behaviour Policy. Teaching about the safe and appropriate use of mobile technologies should be included in the online safety education programme.

# Potential Benefits of Mobile Technologies

Research has highlighted the widespread uptake of mobile technologies amongst adults and children of all ages. Web-based tools and resources have changed the landscape of learning. Students now have at their fingertips unlimited access to digital content, resources, experts, databases and communities of interest. By effectively maximizing the use of such resources, schools not only have the opportunity to deepen student learning, but they can also develop digital literacy, fluency and citizenship in students that will prepare them for the high tech world in which they will live, learn and work.
For further reading, please refer to "Bring your own device: a guide for schools" by Alberta Education available at: http://education.alberta.ca/admin/technology/research.aspx and to the "NEN Technical Strategy Guidance Note 5 – Bring your own device" - http://www.nen.gov.uk/bring-your-own-device-byod/

## Considerations

There are a number of issues and risks to consider when implementing mobile technologies, these include; security risks in allowing connections to your school network, filtering of personal devices, breakages and insurance, access to devices for all students, avoiding potential classroom distraction, network connection speeds, types of devices, charging facilities, total cost of ownership
Schools may consider implementing the use of mobile technologies as a means of reducing expenditure on school provided devices. However, it is important to remember that the increased network management costs and overheads involved in implementing this properly are likely to counterbalance or outweigh any savings.
The use of mobile technologies brings both real benefits and challenges for the whole school community – including teachers - and the only effective way for a school to implement these successfully is to involve the whole school community from the outset. Before the school embarks on this path, the risks and benefits must be clearly identified and shared with all stakeholders.

- The school Acceptable Use Agreements for staff, pupils/students and parents/carers will give consideration to the use of mobile technologies
- The school allows: (the school should complete the table below to indicate which devices are allowed and define their access to school systems)

| | School Devices | | | Personal Devices | | |
|---|---|---|---|---|---|---|
| | School owned and allocated to a single user | School owned for use by | Authorised device[2] | Pupil/Student owned | Staff owned | Visitor owned |

[2] Authorised device – purchased by the pupil/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school

| | | multiple users | | | | |
|---|---|---|---|---|---|---|
| Allowed in school | **Yes** | **Yes** | **Yes** | Yes / No[3] | Yes / No[3] | Yes / No[3] |
| Full network access | *Yes* | *Yes* | *Yes* | | | |
| Internet only | | | | | | |
| No network access | | | | | | |

- **The school has provided technical solutions for the safe use of mobile technology for school devices/personal devices (delete / amend as appropriate):**
  - **All school devices are controlled though the use of Mobile Device Management software**
  - **Appropriate access control is applied to all mobile devices according to the requirements of the user (e.g. Internet only access, network access allowed, shared folder network access)**
  - **The school has addressed broadband performance and capacity to ensure that core educational and administrative activities are not negatively affected by the increase in the number of connected devices**
  - **For all mobile technologies, filtering will be applied to the internet connection and attempts to bypass this are not permitted**
  - **Appropriate exit processes are implemented for devices no longer used at a school location or by an authorised user**. These may include; revoking the link between MDM software and the device, removing proxy settings, ensuring no sensitive data is removed from the network, uninstalling school-licenced software etc.
  - *All school devices are subject to routine monitoring*
  - *Pro-active monitoring has been implemented to monitor activity*
  - *When personal devices are permitted:*
  - *All personal devices are restricted through the implementation of technical solutions that provide appropriate levels of network access*
  - *Personal devices are brought into the school entirely at the risk of the owner and the decision to bring the device in to the school lies with the user (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in school*
  - *The school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover that device whilst out of the home)*
  - *The school accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network or whilst resolving any connectivity issues*
  - *The school recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the school. Pass-codes or PINs should be set on personal devices to aid security*
  - *The school is not responsible for the day to day maintenance or upkeep of the users personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues*
  - **Users are expected to act responsibly, safely and respectfully in line with current Acceptable Use Agreements, in addition;**
  - **Devices may not be used in tests or exams**
  - **Visitors should be provided with information about how and when they are permitted to use mobile technology in line with local safeguarding arrangements**

[3] The school should add below any specific requirements about the use of personal devices in school, e.g. storing in a secure location, use during the school day, liability, taking images etc.

- **Users are responsible for keeping their device up to date through software, security and app updates. The device is virus protected and should not be capable of passing on infections to the network**
- **Users are responsible for charging their own devices and for protecting and looking after their devices while in school**
- **Personal devices should be charged before being brought to school as the charging of personal devices is not permitted during the school day**
- **Devices must be in silent mode on the school site and on school buses**
- **School devices are provided to support learning. It is expected that pupils/students will bring devices to school as required.**
- **Confiscation and searching (England) - the school has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate.**
- **The changing of settings (exceptions include personal settings such as font size, brightness, etc…) that would stop the device working as it was originally set up and intended to work is not permitted**
- **The software / apps originally installed by the school must remain on the school owned device in usable condition and be easily accessible at all times. From time to time the school may add software applications for use in a particular lesson. Periodic checks of devices will be made to ensure that users have not removed required apps**
- **The school will ensure that school devices contain the necessary apps for school work. Apps added by the school will remain the property of the school and will not be accessible to students on authorised devices once they leave the school roll. Any apps bought by the user on their own account will remain theirs.**
- **Users should be mindful of the age limits for app purchases and use and should ensure they read the terms and conditions before use.**
- **Users must only photograph people with their permission. Users must only take pictures or videos that are required for a task or activity. All unnecessary images or videos will be deleted immediately**
- *Devices may be used in lessons in accordance with teacher direction*
- *Staff owned devices should not be used for personal purposes during teaching sessions, unless in exceptional circumstances*
- *Printing from personal devices will not be possible*

# Social Media Policy

Social media (e.g. Facebook, Twitter, LinkedIn) is a broad term for any kind of online platform which enables people to directly interact with each other. However some games, for example Minecraft or World of Warcraft and video sharing platforms such as You Tube have social media elements to them.
*The school* recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents/carers and pupils/students are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by *the school*, its staff, parents, carers and children.

## Scope

**This policy is subject to the school's Codes of Conduct and Acceptable Use Agreements.**
**This policy:**

- **Applies to all staff and to all online communications which directly or indirectly, represent the school.**
- **Applies to such online communications posted at any time and from anywhere.**
- Encourages the safe and responsible use of social media through training and education
- *Defines the monitoring of public social media activity pertaining to the school*

The school respects privacy and understands that staff and pupils/students may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy.
**Professional communications are those made through official channels, posted on a school account or using the school name. All professional communications are within the scope of this policy.**
Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
Digital communications with pupils/students are also considered. *Staff may use social media to communicate with learners via a school social media account for teaching and learning purposes but must consider whether this is appropriate and consider the potential implications.*

## Organisational control

### Roles & Responsibilities

- **SLT**
  - Facilitating training and guidance on Social Media use.
  - Developing and implementing the Social Media policy
  - Taking a lead role in investigating any reported incidents.
  - Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.
  - Receive completed applications for Social Media accounts
  - Approve account creation
- **Administrator / Moderator**
  - Create the account following SLT approval

    - Store account details, including passwords securely
    - Be involved in monitoring and contributing to the account
    - Control the process for managing an account after the lead staff member has left the organisation (closing or transferring)
- **Staff**
    - Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies
    - Attending appropriate training
    - Regularly monitoring, updating and managing content he/she has posted via school accounts
    - Adding an appropriate disclaimer to personal accounts when naming the school

## Process for creating new accounts

The school community is encouraged to consider if a social media account will help them in their work, e.g. a history department Twitter account, or a "Friends of the school" Facebook page. Anyone wishing to create such an account must present a business case to the School Leadership Team which covers the following points:-

- The aim of the account
- The intended audience
- How the account will be promoted
- Who will run the account (at least two staff members should be named)
- Will the account be open or private/closed

Following consideration by the SLT an application will be approved or rejected. In all cases, the SLT must be satisfied that anyone running a social media account on behalf of the school has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the school, including volunteers or parents.

## Monitoring

**School accounts must be monitored regularly and frequently** (preferably 7 days a week, including during holidays). Any comments, queries or complaints made through those accounts must be responded to within 24 hours (or on the next working day if received at a weekend) even if the response is only to acknowledge receipt. Regular monitoring and intervention is essential in case a situation arises where bullying or any other inappropriate behaviour arises on a school social media account.

## Behaviour

- **The school requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.**
- **Digital communications by staff must be professional and respectful at all times and in accordance with this policy**. Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. School social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school.
- Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to school activity.
- If a journalist makes contact about posts made using social media staff must follow the school media policy before responding.
- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.
- The use of social media by staff while at work may be monitored, in line with school policies. *The school permits reasonable and appropriate access to private social media sites. However, where*

*excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken*

- The school will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies, and may take action according to the disciplinary policy.

## Legal considerations

- **Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.**
- **Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.**

## Handling abuse

- When acting on behalf of the school, handle offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, school users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken
- If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported using the agreed school protocols.

## Tone

The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing messages are:

- Engaging
- Conversational
- Informative
- Friendly (on certain platforms, e.g. Facebook)

## Use of images

School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

- **Permission to use any photos or video recordings should be sought in line with the school's digital and video images policy**. If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
- **Under no circumstances should staff share or upload student pictures online other than via school owned social media accounts**
- Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Students should be appropriately dressed, not be subject to ridicule and must not be on any school list of children whose images must not be published.
- If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

## Personal use

- **Staff**
    - Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.

  - Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
  - Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
  - *The school permits reasonable and appropriate access to private social media sites.*
- **Pupil/Students**
  - **Staff are not permitted to follow or engage with current or prior pupils/students of the school on any personal social media network account.**
  - The school's education programme should enable the pupils/students to be safe and responsible users of social media.
  - Pupils/students are encouraged to comment or post appropriately about the school. Any offensive or inappropriate comments will be resolved by the use of the school's behaviour policy
- **Parents/Carers**
  - **If parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.**
  - The school has an active parent/carer education programme which supports the safe and positive use of social media. This includes information on the website.
  - Parents/Carers are encouraged to comment or post appropriately about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's complaints procedures.

## Monitoring posts about the school

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school.
- The school should effectively respond to social media comments made by others according to a defined policy or process.

# Legislation

Schools should be aware of the legislative framework under which this Online Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.
It is recommended that legal advice is sought in the advent of an e safety issue or situation.

## Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

## Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

## Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

## Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

## Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

## Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;

- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

## Trademarks Act 1994

This provides protection for Registered Trademarks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trademarks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

## Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

## Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

## Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

## Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

## Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

## Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an

indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

## Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

## Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

## Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

## Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

## The Education and Inspections Act 2006

Empowers Headteacher, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

## The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data. (see template policy in these appendices and for DfE guidance - http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation)

## The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent / carer to use Biometric systems

### The School Information Regulations 2012

Requires schools to publish certain information on its website:
https://www.gov.uk/guidance/what-maintained-schools-must-publish-online

### Serious Crime Act 2015

Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)

# Links to other organisations or documents

The following links may help those who are developing or reviewing a school online safety policy:

### UK Safer Internet Centre

Safer Internet Centre – http://saferinternet.org.uk/
South West Grid for Learning - http://swgfl.org.uk/
Childnet – http://www.childnet-int.org/
Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline
Internet Watch Foundation - https://www.iwf.org.uk/

### CEOP

CEOP - http://ceop.police.uk/
ThinkUKnow - https://www.thinkuknow.co.uk/

### Others

INSAFE - http://www.saferinternet.org/ww/en/pub/insafe/index.htm
UK Council for Child Internet Safety (UKCCIS) - www.education.gov.uk/ukccis
Netsmartz - http://www.netsmartz.org/

### Tools for Schools

Online Safety BOOST – https://boost.swgfl.org.uk/
360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/

### Bullying / Cyberbullying

Enable – European Anti Bullying programme and resources (UK coordination / participation through SWGfL & Diana Awards) - http://enable.eun.org/
Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/
Scottish Government - Better relationships, better learning, better behaviour - http://www.scotland.gov.uk/Publications/2013/03/7388
DfE - Cyberbullying guidance - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf
Childnet – new Cyberbullying guidance and toolkit (Launch spring / summer 2016) - http://www.childnet.com/new-for-schools/cyberbullying-events/childnets-upcoming-cyberbullying-work
Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm

### Social Networking

Digizen – Social Networking
UKSIC - Safety Features on Social Networks
SWGfL - Facebook - Managing risk for staff and volunteers working with children and young people
Connect safely Parents Guide to Facebook

Facebook Guide for Educators

### Curriculum

SWGfL Digital Literacy & Citizenship curriculum
Glow - http://www.educationscotland.gov.uk/usingglowandict/
Teach Today – www.teachtoday.eu/
Insafe - Education Resources

### Mobile Devices / BYOD

Cloud learn Report Effective practice for schools moving to end locking and blocking
NEN - Guidance Note - BYOD

### Data Protection

Information Commissioners Office:
Your rights to your information – Resources for Schools - ICO
Guide to Data Protection Act - Information Commissioners Office
Guide to the Freedom of Information Act - Information Commissioners Office
ICO guidance on the Freedom of Information Model Publication Scheme
ICO Freedom of Information Model Publication Scheme Template for schools (England)
ICO - Guidance we gave to schools - September 2012 (England)
ICO Guidance on Bring Your Own Device
ICO Guidance on Cloud Hosted Services
Information Commissioners Office good practice note on taking photos in schools
ICO Guidance Data Protection Practical Guide to IT Security
ICO – Think Privacy Toolkit
ICO – Personal Information Online – Code of Practice
ICO Subject Access Code of Practice
ICO – Guidance on Data Security Breach Management
SWGfL - Guidance for Schools on Cloud Hosted Services
LGfL - Data Handling Compliance Check List
Somerset - Flowchart on Storage of Personal Data
NEN - Guidance Note - Protecting School Data

### Professional Standards / Staff Training

DfE - Safer Working Practice for Adults who Work with Children and Young People
Childnet / TDA - Social Networking - a guide for trainee teachers & NQTs
Childnet / TDA - Teachers and Technology - a checklist for trainee teachers & NQTs
UK Safer Internet Centre Professionals Online Safety Helpline

### Infrastructure / Technical Support

Somerset - Questions for Technical Support
NEN - Guidance Note - esecurity

# Glossary of Terms

| | |
|---|---|
| **AUP / AUA** | Acceptable Use Policy / Agreement – see templates earlier in this document |
| **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. |
| **CPD** | Continuous Professional Development |
| **FOSI** | Family Online Safety Institute |
| **ES** | Education Scotland |

| | |
|---|---|
| **HWB** | Health and Wellbeing |
| **ICO** | Information Commissioners Office |
| **ICT** | Information and Communications Technology |
| **ICT Mark** | Quality standard for schools provided by NAACE |
| **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 |
| **ISPA** | Internet Service Providers' Association |
| **IWF** | Internet Watch Foundation |
| **LA** | Local Authority |
| **LAN** | Local Area Network |
| **MIS** | Management Information System |
| **Ofcom** | Office of Communications (Independent communications sector regulator) |
| **TUK** | Think U Know – educational online safety programmes for schools, young people and parents. |
| **VLE** | Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting, |
| **WAP** | Wireless Application Protocol |
| **UKSIC** | UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation. |