# E-Safety Policy

Dane Royd Junior & Infant School

'I want to smile every time I come here,' sums up what pupils think of this outstanding school.
OfSTED Report

**Lead Personnel**: Miss C Kelly, Mr J Davison, Mrs C Ward

**Approval by:** E-Safety Committee

**Policy Date:** 1st January 2021

**Review Date:** 1st January 2022

**Review Frequency:** Annually

## Development / Monitoring / Review of this Policy

This E-Safety policy has been developed by Dane Royd E-Safety Committee made up of:

- Headteacher – Miss C Kelly
- Assistant Headteacher – Mr J Davison
- E-Safety Coordinator – Mrs C Ward
- E-Safety Governor- Mr T Manley
- PTA member/s

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

It is based around the SWGFL policy that is recommended by the safer internet group.

## Schedule for Development / Monitoring / Review

| | |
|---|---|
| This Online Safety policy was approved by the Governing Body / E-safety Committee: | |
| The implementation of this E-Safety Policy will be monitored by the: | *Headteacher – Miss C Kelly*<br>*Assistant Headteacher – Mr J Davison*<br>*E-safety Coordinator- Mrs C Ward* |
| Monitoring will take place at regular intervals: | *At a minimum annually however the policy will be reviewed when required to keep pace with any changes that need reflecting* |
| The Governing Body and E-safety Committee will receive a report on the implementation of the E-Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals: | *Half-termly via the Standards Committee* |
| Should serious online safety incidents take place, the following external persons / agencies should be informed: | *LA Safeguarding Officer, LADO, Police* |

### The school will monitor the impact of the policy using:

- Logs of reported incidents on CPOMs
- Monitoring logs of internet activity (including sites visited) / filtering via NET Support DNA
- Internal monitoring data for network activity via MINT IT Support
- Questionnaires of
    - pupils - annually
    - parents / carers - annually
    - staff – annually

## Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school digital technology systems, both in and out of the school.
The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off the school and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-

bullying or other e-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.
The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate E-Safety behaviour that take place out of school.

# Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school.

## Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors on the E-safety Committee, a sub-committee of the Standards committee, receiving regular information about online safety incidents and monitoring reports. T Manley has taken on the role of E-Safety Governor. The role of the E-Safety Governor will include:

- attendance at E-Safety Committee meetings – Termly as part of the Standards Committee
- regular monitoring of online safety incident logs – Termly as part of the Standards Committee
- regular monitoring of filtering
- reporting to relevant Governors – when/where necessary

## Headteacher and Senior Leaders - Miss C Kelly and Mr J Davison

- 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 E-Safety Coordinator – Mrs C Ward.
- The Headteacher and (at least) another member of the Senior Leadership 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. (Flow chart on dealing with online safety incidents can be found in this policy)
- The Headteacher is responsible for ensuring that the E-Safety Coordinator 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 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. This will take place via two members of staff being present when dealing with any technical changes to the system and reports of the monitoring and filtering systems being sent to at least 2 members of the E-Safety committee. The school will also ensure that MINT IT Support have a robust system for checking their staff and work carried out on the network.
- The Headteacher will liaise regularly with the E-Safety Coordinator to check the policy is being implemented fully and consistently.

- The Headteacher/Assistant Headteacher will carry out any investigations regarding breaches of this policy

## E-Safety Coordinator - Mrs C Ward

- leads the E-Safety Committee
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school technical staff
- receives reports of online safety incidents, via CPOMS, and has access to logs of incidents to inform future online safety developments,
- meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs / reports regularly to Headteacher
- The E-safety Coordinator will be responsible for following incidents that involve children and their online safety
- The E-Safety Coordinator will not be responsible for carrying out investigations into staff members – this will be carried out by Assistant Headteacher Mr J Davison.

## Technical staff – MINT IT Support

The Technical Staff (MINT IT Support) 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 the filtering policy is applied and that its implementation is not the sole responsibility of any single person (see appendix "Technical Security Policy Template" for good practice)
- that they keep up to date with 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 and email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation, action and sanction when necessary
- that monitoring software and systems are implemented and updated as agreed in school

## 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* E-Safety Policy and practices

- they have read, understood and signed the Staff Acceptable Use Policy
- they report any suspected misuse or problem to the Headteacher for investigation, action and when necessary sanction
- all digital communications with pupils should be on a professional level and only carried out using official school systems (monitored email and TEAMS)
- all digital communications with parents and carers should be on a professional level and only carried out using official school systems (email/ParentMail)
- Official school systems* include but may not be limited to personal mobile telephone (number withheld) school email, Parentmail, school website, Twitter, Microsoft Teams, Key Stage You Tube Channel, Evidence Me (early years only) Whatsapp (staff group) Facebook (PTA group).
- The school recognises that many staff live in the community and have parents as friends and they should refer to the social media policy for advice on best practice in this area)
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the E-Safety Policy and acceptable use policies
- 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 Leads - Miss C Kelly, Mrs G Kendall, and Mrs A White

Should be trained in E-Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

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

## E-Safety Committee - Miss C Kelly, Mr J Davison, Mrs C Ward, Mr T Manley, PTA Member/s

The E-Safety Committee provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring the E-Safety Policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body.
Members of the E-Safety Committee will assist the E-Safety Coordinator with:

- the production, review and monitoring of the school E-Safety Policy.
- the production, review and monitoring of the school Acceptable User Agreements.
- the production, review and monitoring of the school filtering policy (if the school chooses to have one) and requests for filtering changes.

- mapping and reviewing the E-safety and digital literacy curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs via CPOMs
- consulting stakeholders – including parents / carers and the pupils - about the online safety provision

## Pupils:

- are responsible for using the school digital technology systems in accordance with the 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 online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

## Parents and Carers:

Parents and 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 assemblies, consultation evenings, newsletters, letters, the school website/ Twitter feed and information about national / local online safety campaigns / literature and sign posting to the most up to date information. 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 and school Twitter
- their children's personal devices in the school – see mobile devices policy for further information

## Community Users:

Community Users who access school systems / Twitter feed and PTA Facebook group as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems.

# Policy Statements

## Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety / digital literacy is therefore an essential part of the school's online safety provision. Children and young people 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 will be provided as part of Computing / PHSE / other lessons and will be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
- Pupils will be taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils will 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 at an age appropriate level in accordance with the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet.
- Pupils will be helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff will act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit. (This will be done by having a policy of as many screens on show as possible and teachers and support staff taking a helicopter approach to the lesson)

## Education – Parents and 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 online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters
- Newsletters
- The school website and Twitter Feed
- Consultation evenings
- High profile events and campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

# 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. An audit of the online safety training needs of all staff will be carried out annually
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school E-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 E-Safety Coordinator will receive regular updates through attendance at external training events (e.g. from LA and other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This E-Safety Policy and its updates will be presented to and discussed by staff in staff meetings and INSET days.
- The E-Safety Coordinator will provide advice, guidance and training to individuals as required.

# Training – Governors

Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of the E-Safety Committee or involved in technology online safety, health and safety and safeguarding. This may be offered in a number of ways:

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

# Technical – infrastructure / equipment, filtering and monitoring

The MINT IT Support will be responsible for ensuring that the school infrastructure and network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy is 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:
A more detailed Technical Security Template Policy can be found in the appendix.

- 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
- All users will have clearly defined access rights to school technical systems and devices.
- All users at KS2 and above will be provided with a username and secure password by MINT IT Support who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- The "master / administrator" passwords for the school ICT systems, 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 (eg school safe)
- MINT IT Support 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. There is a clear process in place to deal with requests for filtering changes.
- Internet filtering / monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The school has provided enhanced and differentiated user-level filtering allowing different filtering levels for different ages and different groups of users – staff and pupils
- School technical staff regularly monitor and record the activity of users via NET Support DNA on the school technical systems and users are made aware of this in the Acceptable Use Agreement. E-safety coordinator must meet weekly to check and record a log of the conversation.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed. (First to Headteacher then to MINT Support via the telephone logging incident number)
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts that might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place (Device Loan Agreement) regarding the extent of personal use that users (staff / 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 (Acceptable Use Policy) that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place (stated below) regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. **Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured**. (see School Personal Data Policy Template in the appendix for further detail)

# Mobile Technologies – Staff and Volunteers

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 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.

- The school Acceptable Use Agreements for staff 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** | **Staff owned** | **Visitor owned** |
| Allowed in school | *Yes* | *Yes* | *Yes* | *Yes* | *No* |
| Full network access | *Yes* | *Yes* | *Yes* | *No* | *No* |
| Internet only | | | | *No* | *No* |
| No network access | | | | | |

All teaching staff have been issued with an IPad below is the agreed terms of use:

- IPads can be used for all admin duties required e.g. register and dinner recording
- They can be taken out of school for trips – Password protect
- Personal use is allowed in line with the staff user agreement
- They are subject to inspection, monitoring and filtering
- Installation of apps and changing of settings are communicated to the technical support staff – MINT Support
- If used to access e-mail or cloud based storage they are password protected
- They are used in accordance to the GDPR Policy
- They can be used for capturing curriculum coverage
- They should not be used by any relative or friends

Staff are allowed personal devices and below outlines how they should be used:

- Staff are allowed access to their devices but should use appropriately in school e.g. not be visible in lesson or when pupils are around unless in extreme circumstances such as implementing lockdown procedures

- Devices should be password protected
- They must not be used to record any images, sound or video in school
- Staff can access work emails on their personal devices
- Staff should not access the school network on their personal devices
- Technical support is not available for personal devices
- Filtering of the internet will be the same level as required by the filtering system and staff should be aware their internet will be monitored via the school system
- If any allegations or breaches of the policy are made they will be subject to the procedures set out in this policy

## Mobile Technologies - Pupils

The Mobile devices policy sets out in full the schools position and the procedures if they are breached.

## Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and 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 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 pupils are published on the school website / social media / local press
- 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 pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that 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 pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or Twitter, particularly in association with photographs.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

# Data Protection

Please see Privacy notice for parents
Privacy notice for staff
Records Management Policy
Data Retention Policy

# Communications

Dane Royd is a wholly inclusive school, as such it has invested in all the appropriate technology to support the teaching of a rich and varied curriculum. Below is a table demonstrating how this equipment may be used:

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

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.
- Users must immediately report, to the nominated person (Headteacher), 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 pupils or parents / carers regarding school (email, social media, chat, etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems e.g. Email, parent mail or official Facebook group monitored by Headteacher. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils will 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

Please see Social Media Policy

# Dealing with 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 / academy | | | | | 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 | |

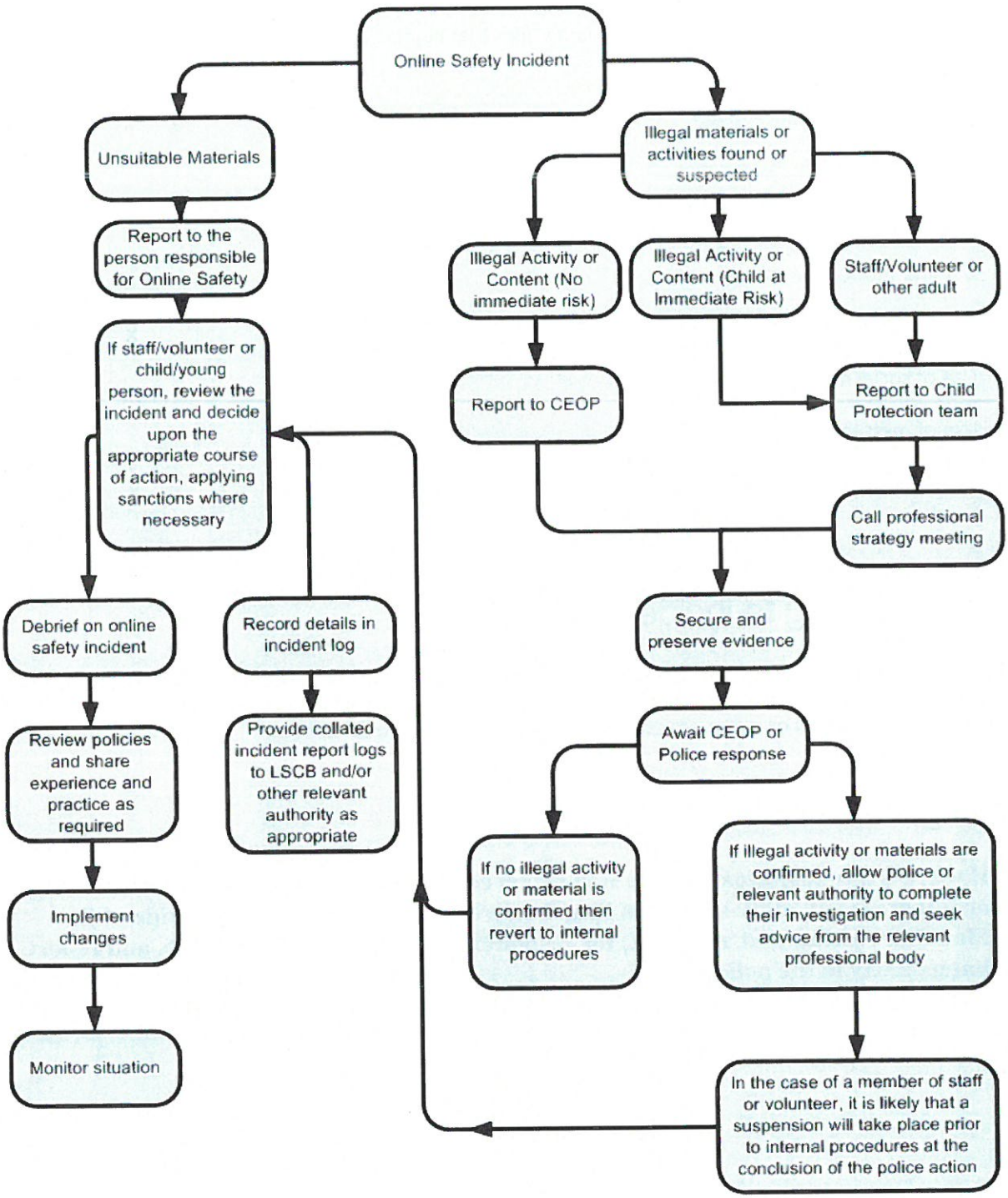
| | | | | | |
|---|---|---|---|---|---|
| Unfair usage (downloading / uploading large files that hinders others in their use of the internet) | | | | X | |
| On-line gaming (educational) | | x | | | |
| On-line gaming (non-educational) | | | x | | |
| On-line gambling | | | x | | |
| On-line shopping / 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 staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

# Illegal Incidents

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


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

# Other Incidents

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

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

- Have more than one senior member of staff 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 using the reporting format found in the Appendicies. 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 (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.

# School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour procedures but could result in the following depending on severity:

| Pupils Incidents | Refer to class teacher | 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 | Warning | Further sanction e.g 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 | x | x | x | x |
| Unauthorised use of non-educational sites during lessons | x | | | | x | | | |
| Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device | x | x | | | x | x | x | x |
| Unauthorised / inappropriate use of social media / messaging apps / personal email | x | x | | | x | x | x | x |
| Unauthorised downloading or uploading of files | x | | | x | x | x | x | x |
| Allowing others to access school network by sharing username and passwords | x | x | | x | x | x | x | X |
| Attempting to access or accessing the school network, using another pupil's account | x | x | | | x | x | x | x |
| Attempting to access or accessing the network, using the account of a member of staff | x | x | | x | x | x | x | x |
| Corrupting or destroying the data of other users | x | x | | x | x | x | x | X |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | x | x | x | x | x | x | x | x |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school | x | x | x | x | x | x | x | X |
| Using proxy sites or other means to subvert the school's x filtering system | x | x | x | | x | x | x | x |
| Accidentally accessing offensive or pornographic material and failing to report the incident | x | x | x | | x | x | x | x |
| Deliberately accessing or trying to access offensive or pornographic material | x | x | x | x | x | x | x | x |
| Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act | x | x | x | | | x | x | x |

| Staff Incidents | 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 | x | x |
| Inappropriate personal use of the internet / social media / personal email | X | | x | x | x | x |
| Unauthorised downloading or uploading of files | x | | x | x | x | x |
| 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 | x | | x | x | x | x |
| Careless use of personal data e.g. holding or transferring data in an insecure manner | x | | x | x | x | x |
| Deliberate actions to breach data protection or network security rules | x | | x | x | x | x |

| | | | | | | |
|---|---|---|---|---|---|---|
| Corrupting or destroying the data of other users or causing deliberate damage to hardware or software | x | | x | x | x | x |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | x | | x | x | x | x |
| Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils | x | x | x | x | x | x |
| Actions which could compromise the staff member's professional standing | x | | x | x | x | X |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school | x | | x | x | x | x |
| Using proxy sites or other means to subvert the school's / filtering system | x | | x | x | x | x |
| Accidentally accessing offensive or pornographic material and failing to report the incident | x | | x | x | x | x |
| Deliberately accessing or trying to access offensive or pornographic material | x | | x | x | x | x |
| Breaching copyright or licensing regulations | x | | x | x | x | x |
| Continued infringements of the above, following previous warnings or sanctions | x | x | x | x | x | x |

# Appendices

**Pupil Acceptable Use Agreement**

School Policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These 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. Young people should have an entitlement to safe internet access at all times.

*This Pupil Acceptable Use Agreement is intended to ensure:*

- that pupil's will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse, will have good access to digital technologies to enhance their learning and will, in return, agree to be responsible users.

**Pupil Acceptable Use Agreement – for older pupils (LSK2 / UKS2)**

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.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, 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 not disclose or share personal information about myself or others when on-line (this could include full names, home addresses, email addresses, telephone numbers, age/date of birth, gender, educational details, financial details etc.)
- I will be aware of "stranger danger", when I am communicating on-line.
- If I arrange to meet people off-line that I have communicated with on-line, I will take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will only use Microsoft Teams (a powerful collaborative working and communication tool available within the Microsoft Office 365 environment) for curriculum related content, discussion and support.
- 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 use the school systems or devices to access social media sites (e.g. Facebook), on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube).

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will not take or distribute images of anyone without their permission.
- I will be polite and responsible when I communicate with others
- I appreciate that others may have different opinions and will not use strong, aggressive or inappropriate language towards others.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will not use my own personal devices (mobile phones / USB devices etc.) in school unless I have explicit permission from the Headteacher.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I 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 damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, 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 not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will not use social media sites.

When using the internet for research or recreation, I recognise that:

- I should 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 try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Pupil Acceptable Use Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

**Pupil Acceptable Use Agreement – for older pupils (LSK2 / UKS2)**

Please complete the sections below to show that you have read, understood and agree to the rules included in the Pupil 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

Name of Pupil: .....

Class: .....

Signed: .....

Date: .....

**Pupil Acceptable Use Agreement – 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 laptops / ipads
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of the electronic 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 laptops / ipads in future

Class: .....

Date: .....

Pupil Signatures (below):

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

**Staff (and Volunteer) Acceptable Use Agreement**

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communication 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 Staff (and Volunteer) Acceptable Use Agreement 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 systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff (and volunteers) 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 pupils learning and will, in return, expect staff (and volunteers) to agree to be responsible users.

**Staff (and Volunteer) Acceptable Use 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 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 including staff e-mails.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, 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.
- 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 / Twitter) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils and parents / carers about school using official school systems –including but may not be limited to personal mobile telephone (number withheld) school email, Parentmail, school website, Twitter, Microsoft Teams, Key Stage You Tube Channel, Evidence Me (early years only) Whatsapp (staff group) Facebook (PTA group).
- Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibility.

*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 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.
- 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 and 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 pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

*When using the internet in my professional capacity or for 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 Staff (and Volunteer) Acceptable Use Agreement applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school 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 Staff (and Volunteer) Acceptable Use Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors / Directors and / or the Local Authority and in the event of illegal activities the involvement of the police.

**Staff (and Volunteer) Acceptable Use Agreement**

Please complete the sections below to show that you have read, understood and agree to the rules included in the Staff (and Volunteer) 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 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 - Please respond to HR Manager's email using vote button provided.**

**Volunteers**

Name: .....

Position: .....

Signed: .....

Date: .....

## 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* | |
|---|---|
| | |
| | |

## Training needs audit log to be carried out annually.

| Training Needs Audit Log<br>Group: ..... | | | | |
|---|---|---|---|---|
| *Relevant training the last 12 months* | *Identified Training Need* | *To be met by* | *Cost* | *Review Date* |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# School Technical Security Policy (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 MINT IT Support 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 MINT IT Support

# Technical Security

## Policy statements

MINT IT Support 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, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff
- 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 / Technical Staff (or other person) and will be reviewed, at least annually, by the E-Safety Committee
- 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. (See Password section below).

- MINT IT Support 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 – all computers/USB are BIT Lockered and password protected
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- Remote management tools are used by staff to control workstations and view users activity
- An appropriate system is in place for users to report any actual / potential technical incident to the E-Safety Coordinator / Network Manager / Technician (or other relevant person, as agreed

- An agreed policy is in place 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* (in user agreement) *regarding the downloading of executable files and the installation of programmes on school devices by users*
- *An agreed policy is in place* (in device loan agreement) *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* (in user agreement) *regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices.* (see School Personal Data Policy Template in the appendix for further detail)
- 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. (see School Personal Data Policy Template in the appendix for further detail)

# 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 and email

## 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 E-Safety Group (or other group).
- All school networks and systems will be protected by secure passwords.
- The "master / administrator" passwords for the school systems, used by the technical staff must also be available to the Headteacher but are held by staff.
- 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 MINT IT Support. Any changes carried out must be notified to the manager of the password security policy (above).
- Users will change their passwords at regular intervals – as described in the staff and pupil sections below
- Where passwords are set / changed manually requests for password changes should be authenticated by MINT IT Support to ensure that the new password can only be passed to the genuine user

## Staff Passwords

- All staff users will be provided with a username and password by Mint Support Ltd who 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
- must not include: Password, Admin, Dane, Royd
- 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 not re-used for 6 months and be significantly different from previous passwords created by the same user.

## Pupil Passwords

- All users at KS2 and above will be provided with a username and password by MINT IT Support who will keep an up to date record of users and their usernames.
- Pupils will be taught the importance of password security
- *School* password routines should model good password practice for users
- The complexity (i.e. minimum standards) will be set with regards to the cognitive ability of the children

## Training / Awareness

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

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

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

- in lessons
- through the Acceptable Use Agreement

## Audit / Monitoring / Reporting / Review

Mint Support Ltd will ensure that full records 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 Mint Support Ltd They 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
- be reported to a second responsible person (Headteacher) prior to changes being made

All users have a responsibility to report immediately to MINT IT Support 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 lists . 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.

- The school maintains and supports the managed filtering service provided by the Internet Service Provider
- The school has provided enhanced / differentiated user-level filtering through the use of the RM user based filtering programme. (allowing different filtering levels for different ages / stages and different groups of users – staff / pupils 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
- Mobile devices that access the school internet connection (whether school 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 Mint Support Ltd If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Committee.

## Education / Training / Awareness

Pupils will be made aware of the school's filtering systems through:

- Acceptable Use Agreement
- online safety education programme
- They will also be warned of the consequences of attempting to subvert the filtering system.

Staff will be made aware of the school's filtering systems through:

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

Parents will be made aware of the school's filtering policy through:

- Acceptable Use Agreement
- online safety awareness sessions, newsletters, website and assemblies etc.

## Changes to the Filtering System

Any requests to change the filtering system should be made to Mint Support Ltd and be signed off by the Headteacher. These requests should have a strong educational reason and may be denied. Any changes will be reported to the E-Safety Coordinator to be logged. This should record who requested the change, who authorised the change and for how long it will be in effect.

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 the Headteacher who will decide whether to make school level changes (as above).

# 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 E-Safety Policy and the Acceptable Use Agreement. Monitoring will take place as follows:

- Mint Support Ltd will monitor the network and infrastructure
- NETSupport DNA will monitor user activity on the network: E-Safety Coordinator
  Headteacher
  Deputy Headteacher
  Assistant Headteacher

Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- the second responsible person (Headteacher)
- E-Safety Committee
- E-Safety Governor
- 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.

# School Policy: Electronic Devices - Searching & Deletion

The Education Act 2012, the basis of this policy, sets out what the law is presumed to be, based on prior legal and educational knowledge, and common sense. Rights and responsibilities regarding physical contact and personal data are still evolving rapidly. So too are social, entertainment and educational technologies and the skills necessary to use them safely and prudently. This is particularly so where those who are under 18 are involved.
No existing law or policy can fully insulate anyone from the risk involved in searching for, access to or deletion of the personal data of others. Anyone refraining from any such search, access or deletion when hindsight shows circumstances merit such actions may however be at significant risk and may put seriously at risk the wellbeing of children entrusted to their care. This policy cannot therefore be relied on as justification for any act or lack of action by anyone – there is no substitute for the proper and well documented exercise of adequately informed professional judgement. .

## Introduction

The changing face of information technologies and ever increasing pupil 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 Headteacher must publicise the school behaviour policy, in writing, to staff, parents and carers and pupils at least once a year.

## 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 Governors 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: Mr J Davison/ Miss C Kelly and Mrs E Wake

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:
Miss C Kelly – Headteacher
Mrs G Kendall – Deputy Headteacher

Mr J Davison- Assistant Headteacher
Mrs E Wake – HR Manager

The Headteacher may authorise other staff members in writing in advance of any search they may undertake, subject to appropriate training however, members of staff cannot be required to carry out such searches. They can each choose whether or not they wish to be an authorised member of staff.

## Training / Awareness

It is essential that all staff should be made aware of and should implement the school's policy.

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 E-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. Pupils are not allowed to bring mobile phones or other personal electronic devices to school or use them in the school. If pupils breach this rule consequences will be issued and can be found in the Behaviour Policy and Mobile Devices 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 *pupil* is in possession of a prohibited item i.e. an item banned by the school rules and which can be searched for.
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. (NB :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.)
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 pupil being searched.
The authorised member of staff carrying out the search must be the same gender as the *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 *pupil* being searched.

There is a limited exception to this rule: Authorised staff can carry out a search of a 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 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 pupil has or appears to have control – this includes desks, lockers and bags. (NB: school will need to take account of normal policies regarding religious garments / headwear)
A pupil's possessions can only be searched in the presence of the 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
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 through DSL training. Care should be taken not to delete material that might be required in a potential criminal investigation.

The school will consider our 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 are arrangements in place to support such staff.

Further guidance on reporting the incident to the police and the preservation of evidence can be found in the flow chart in the main E-Safety Policy.

## 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.

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.

A record should be kept of the reasons for the deletion of data / files on CPOMs in the Incident report section.

## Care of Confiscated Devices

The school cannot be held liable for damage to confiscated items. Any items brought to school are at parents risk as stated in the behaviour policy.

## Audit / Monitoring / Reporting / Review

The Headteacher 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.
These records will be reviewed by E-Safety Committee half termly.
This policy will be reviewed by the head teacher and governors 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

## Further Guidence for staff implementing this 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" (2014 and updated January 2018)
http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation
It is recommended that Headteachers / Principals (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

This is not a full list of Acts involved in the formation of this advice. Further information about relevant legislation can be found via the above link to the DfE advice document.

# Device loan agreement for pupils

## 1. This agreement is between:

1) Dane Royd Junior and Infant School

2) Name of Parent:

Address of Parent:

And governs the use and care of devices assigned to the parent's child ( the "pupil"). This agreement covers the period from the date the device is issued through to the return date of the device to the school.

All issued equipment shall remain the sole property of the school and is governed by the school's policies.

1. The school is lending the pupil a laptop ("the equipment") for the purpose of accessing remote learning during the lockdown.
2. This agreement sets the conditions for taking a Dane Royd laptop ("the equipment")] home.

**I confirm that I have read the terms and conditions set out in the agreement and my signature at the end of this agreement confirms that I and the pupil will adhere to the terms of loan.**

## 2. Damage/loss

By signing this agreement I agree to take full responsibility for the loan equipment issued to the pupil and I have read or heard this agreement read aloud and understand the conditions of the agreement.

I understand that I and the pupil are responsible for the equipment at all times whether on the school's property or not.

If the equipment is damaged, lost or stolen, I will immediately inform Miss Kelly and I acknowledge that I am responsible for the reasonable costs requested by the school to repair or replace the equipment. If the equipment is stolen, I will also immediately inform the police.

I agree to keep the equipment in good condition and to return it to the school on their demand from the school in the same condition.

I will not leave the equipment unsupervised in unsecured areas.

I will make sure my child takes the following measures to protect the device:

- Keep the device in a secure place when not in use
- Don't leave the device in a car or on show at home
- Don't eat or drink around the device
- Don't lend the device to siblings or friends
- Don't leave the equipment unsupervised in unsecured areas

## 3. Unacceptable use

I am aware that the school monitors the pupil's activity on this device.

I agree that my child will not carry out any activity that constitutes 'unacceptable use'.

This includes, but is not limited to the following:

- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Causing intentional damage to ICT facilities or materials
- Using inappropriate or offensive language

I accept that the school will sanction the pupil, in line with our behaviour policy if the pupil engages in any of the above **at any time.**

## 4. Personal use

I agree that the pupil will only use this device for educational purposes and not for personal use and will not loan the equipment to any other person.

## 5. Data protection

I agree to take the following measures to keep the data on the device protected.

- Keep the equipment password-protected with the password provided by school and do not change the password
- Make sure my child locks the equipment if it's left inactive for a period of time
- Do not share the equipment among family or friends
- Update antivirus and anti-spyware software as required
- Install the latest updates to operating systems, as prompted

If I need help doing any of the above, I will contact Dane Royd School on the email headteacher@daneroyd.wakefield.sch.uk

## 6. Return date

I will return the device in its original condition to Dane Royd School within 5 days of being requested to do so.

I will ensure the return of the equipment to the school if the pupil no longer attends the school.

## 7. Consent

By signing this form, I confirm that I have read and agree to the terms and conditions set out above. (if laptop collected in person)

| | |
|---|---|
| PUPIL'S FULL NAME | |
| PARENT'S FULL NAME | |
| PARENT'S SIGNATURE | |

## Links to other organisations or documents

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

UK Safer Internet Centre

Safer Internet Centre – https://www.saferinternet.org.uk/

South West Grid for Learning - https://swgfl.org.uk/products-services/online-safety/

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

LGfL – Online Safety Resources

Kent – Online Safety Resources page

INSAFE / Better Internet for Kids - https://www.betterinternetforkids.eu/

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/

360Data – online data protection self review tool: www.360data.org.uk

Bullying / Online-bullying / Sexting / Sexual Harrassment

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 – Cyberbullying guidance and practical PSHE toolkit: http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit

Childnet – Project deSHAME – Online Sexual Harrassment

UKSIC – Sexting Resources

Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm

Ditch the Label – Online Bullying Charity

Diana Award – Anti-Bullying Campaign

Social Networking

Digizen – Social Networking

UKSIC - Safety Features on Social Networks

Children's Commissioner, TES and Schillings – Young peoples' rights on social media

Curriculum

SWGfL Digital Literacy & Citizenship curriculum

UKCCIS – Education for a connected world framework

Teach Today – www.teachtoday.eu/

Insafe - Education Resources

Mobile Devices / BYOD

Cloudlearn Report Effective practice for schools moving to end locking and blocking

NEN - Guidance Note - BYOD

Data Protection

360data - free questionnaire and data protection self review tool

ICO Guide for Organisations (general information about Data Protection)

ICO Guides for Education (wide range of sector specific guides)

DfE advice on Cloud software services and the Data Protection Act

ICO Guidance on Bring Your Own Device

ICO Guidance on Cloud Computing

ICO - Guidance we gave to schools - September 2012

IRMS - Records Management Toolkit for Schools

NHS - Caldicott Principles (information that must be released)

ICO Guidance on taking photos in schools

Dotkumo - Best practice guide to using photos

Professional Standards / Staff Training

DfE – Keeping Children Safe in Education

DfE - Safer Working Practice for Adults who Work with Children and Young People

Childnet – School Pack for Online Safety Awareness

UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure / Technical Support

UKSIC – Appropriate Filtering and Monitoring

Somerset - Questions for Technical Support

NEN – Advice and Guidance Notes

Working with parents and carers

SWGfL Digital Literacy & Citizenship curriculum

Online Safety BOOST Presentations - parent's presentation

Vodafone Digital Parents Magazine

Childnet Webpages for Parents & Carers

Get Safe Online - resources for parents

Teach Today - resources for parents workshops / education

The Digital Universe of Your Children - animated videos for parents (Insafe)

Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide

Insafe - A guide for parents - education and the new media

Research

EU Kids on Line Report - "Risks and Safety on the Internet" - January 2011

Futurelab - "Digital participation - its not chalk and talk any more!"

Ofcom –Media Literacy Research

## 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 |
| **ICO** | Information Commissioners Office |
| **ICT** | Information and Communications Technology |
| **ICTMark** | 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 |
| **NEN** | National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain. |
| **Ofcom** | Office of Communications (Independent communications sector regulator) |
| **SWGfL** | South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW |
| **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. |