# Online Safety Policy

| | |
|---|---|
| **Version** | 3 |
| **Approved on:** | 21/03/2024 |
| **Update frequency (years)** | 2 |
| **Date of next review** | 21/03/2026 |

Contents


Development / Monitoring / Review of this Policy 4
Schedule for Development / Monitoring / Review 4
Scope of the Policy 5
Roles and Responsibilities 5
Governors / Board of Directors: 5
Headteacher and Senior Leaders: 5
Online Safety Coordinator: 6
Network Manager / Technical staff: 6
Teaching and Support Staff 6
Designated Safeguarding Lead / Officer 7
Online Safety Group 7
Pupils: 8
Parents / Carers 8
Community Users 8
Policy Statements 8
Education – Pupils 8
Education – Parents / Carers 9

Education – The Wider Community 9
Education & Training – Staff / Volunteers 10
Training – Governors 10
Technical – infrastructure / equipment, filtering and monitoring 10
Mobile Technologies (including BYOD/BYOT) 12
Use of digital and video images 14
Data Protection 14
Communications 16
Staff / adults 16
Students / Pupils 16
Social Media - Protecting Professional Identity 17
Unsuitable / inappropriate activities 18
Responding to incidents of misuse 19
Reparative 19
Illegal Incidents 20
Other Incidents 21
School Actions & Sanctions 21

# Development / Monitoring / Review of this Policy

This Online Safety policy has been developed by a working group / committee made up of:

- Senior Leaders
- Online Safety Coordinator
- Staff – including Teachers, Support Staff, Technical staff
- Governors
- Parents and Carers
- Community users
- Digital Leaders

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

# Schedule for Development / Monitoring / Review

| | |
|---|---|
| The implementation of this Online Safety policy will be monitored by the: | *Online Safety Committee* |
| Monitoring will take place at regular intervals: | *Bi-annually* |
| The Governing Body will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals: | *Annually* |
| 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
- Monitoring logs of internet activity (including sites visited) / filtering
- Internal monitoring data for network activity
- Surveys / questionnaires of
    - students / pupils
    - parents / carers
    - staff

# Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act

increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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 Online Safety behaviour that take place out of school.

# Online Safety Statutory Duties

Extracts from Keeping Children Safe In Education September 2018 (National Online Safety Centre)

**Online Safety - Page 22 Paragraph 84**

84. As schools and colleges increasingly work online, it is essential that children are safeguarded from potentially harmful and inappropriate online material. As such, governing bodies and proprietors should ensure appropriate filters and appropriate monitoring systems are in place. Additional information to support governing bodies and proprietors keep their children safe online is provided in Annex C.

**Opportunities to teach safeguarding - Page 22 Paragraph 85, 86 & 87**

85. Governing bodies and proprietors should ensure that children are taught about safeguarding, including online safety. Schools should consider this as part of providing a broad and balanced curriculum.

86. This may include covering relevant issues through Relationships Education and Relationships and Sex Education (formerly known as Sex and Relationship Education), tutorials (in colleges) and/or where delivered, through Personal, Social, Health and Economic (PSHE) education.

87. Whilst it is essential that governing bodies and proprietors ensure that appropriate filters and monitoring systems are in place, they should be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding.

**Sexual violence and sexual harassment between children in schools and colleges - Page 6**

Specific online references include:

- Children who are victims of sexual violence and sexual harassment will likely find the experience stressful and distressing. This will, in all likelihood, adversely affect their educational attainment. Sexual violence and sexual harassment exist on a continuum and may overlap, they can occur online and offline (both physically and verbally) and are never acceptable. It is important that all victims are taken seriously and offered appropriate support.

Online sexual harassment, page 10

- This may be standalone, or part of a wider pattern of sexual harassment and/or sexual violence.
- It may include: • non-consensual sharing of sexual images and videos. (UKCCIS sexting advice provides detailed advice for schools and colleges); • sexualised online bullying; • unwanted sexual comments and messages, including, on social media; and • sexual exploitation; coercion and threats.

Harmful sexual behaviour, page 10
Harmful sexual behaviour can occur online and/or offline and can also occur simult

**Preventing radicalisation - page 83**

Background factors combined with specific influences such as family and friends may contribute to a child's vulnerability. Similarly, radicalisation can occur through many different methods (such as social media) and settings (such as the internet).

**Annex B: The role of the designated safeguarding lead - Training - Page 90**

• are able to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college;

• can recognise the additional risks that children with SEN and disabilities (SEND) face online, for example, from online bullying, grooming and radicalisation and are confident they have the capability to support SEND children to stay safe online;

**Annex C: Online Safety - page 93**

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate. The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

• content: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;

• contact: being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and

• conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

Filters and monitoring

Governors and proprietors should ensure that, as part of the requirement for staff to undergo regularly updated safeguarding training (paragraph 81) and the requirement 112 The Prevent duty Departmental advice for schools and childcare providers and Prevent Duty Guidance For Further Education Institutions 95 to ensure children are taught about safeguarding, including online safety (paragraph 85), that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach.

The appropriateness of any filters and monitoring systems are a matter for individual schools and colleges and will be informed in part, by the risk assessment required by the Prevent Duty. 112 The UK Safer Internet Centre has published guidance as to what "appropriate" filtering and monitoring might look like: UK Safer Internet Centre: appropriate filtering and monitoring.

Guidance on e-security is available from the National Education Network. Support for schools is available via the: schools' buying strategy with specific advice on procurement here: buying for schools. Whilst filtering and monitoring is an important part of the online safety picture for schools and colleges to consider, it is only one part. Governors and proprietors should consider a whole school or college approach to online safety. This will include a clear policy on the use of mobile technology in the school or college. Many children have unlimited and unrestricted access to the internet via 3G and 4G in particular and the school and college should carefully consider how this is managed on their premises.

Whilst it is essential that governing bodies and proprietors ensure that appropriate filters and monitoring systems are in place, they should be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding.

Staff training

Governors and proprietors should ensure that, as part of the requirement for staff to undergo regularly updated safeguarding training (paragraph 81) and the requirement 112 The Prevent duty Departmental advice for schools and childcare providers and Prevent Duty Guidance For Further Education Institutions 95 to ensure children are taught about safeguarding, including online safety (paragraph 85), that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach.

# Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within Westhaven School.

## Governors:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Coordinator
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors

## Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including Online Safety) of members of the school community, though the day to day responsibility for Online Safety will be delegated to the Online Safety Coordinator.
- 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. (see flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR disciplinary procedures).
- The Headteacher and Senior Leaders are responsible for ensuring that the Online 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 / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role (Smoothwall / CPOMS or similar). This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Coordinator.

## Online Safety Coordinator:

- leads the Online Safety Group
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- 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 / relevant body
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments, meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / Governor meetings
- reports regularly to Senior Leadership Team

## Network Manager / Technical staff:

The Network Manager 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 that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- 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 / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher and Online Safety Coordinator for investigation / action / sanction
- that monitoring systems are implemented and updated as agreed in school policies

# Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Online Safety Coordinator via a Level 2 Behaviour Form for investigation / action / sanction
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online Safety Policy and Acceptable Use Policy
- 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 pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

# Designated Safeguarding Lead / Officer

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

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

# Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the

impact of initiatives. Depending on the size or structure of the school this group may be part of the safeguarding group. The group will also be responsible for regular reporting to the Governing Body.

Members of the Online Safety Group (or other relevant group) will assist the Online Safety Coordinator with:

- the production / review / monitoring of the school Online Safety Policy / documents.
- the production / review / monitoring of the school filtering policy and requests for filtering changes.
- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the pupils about the online safety provision
- monitoring improvement actions identified through use of the 360 degree safe self-review tool

## 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 cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school

## Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to

support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website and online student / pupil records
- their children's personal devices in the school (where this is allowed)

## Community Users

Community Users who access school systems / website as part of the wider school provision will be expected to sign a Community User AUP 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 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 (SWGfL Digital Literacy curriculum/ Google Be Internet Legends / Purple Mash or similar) should be provided as part of Computing other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Pupils should 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 should act as good role models in their use of digital technologies the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that 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.

- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

## Education – Parents / Carers

Many parents and carers have only a limited understanding of 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, web site
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant websites / publications

## Education – The Wider Community

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

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

# Education & Training – Staff / Volunteers

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

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Coordinator will receive regular updates through attendance at external training events (eg from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Online Safety Coordinator (or other nominated person) will provide advice / guidance / 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 any group involved in technology / online safety / health and safety /safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation (e.g. SWGfL).
- Participation in school training / information sessions for staff or parents

# Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the

relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- The school's 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 / academy technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school / academy technical systems and devices.
- All users will be provided with a username and secure password by the Network Manager. Users are responsible for the security of their username and password and will be required to change their password if there is a possible security breach / incident.
- The "master / administrator" passwords for the school / academy ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (eg school / academy safe)
- The Network Manager 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 should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The school has provided enhanced / differentiated user-level filtering
- 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 (Smoothwall Monitor or similar)
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date antivirus 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 regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place that forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place 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.

# Mobile Technologies (including BYOD/BYOT)

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

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

| | School Devices | | | Personal Devices | | |
|---|---|---|---|---|---|---|
| | School owned for single user | School owned for multiple users | Authorised device | Student owned | Staff owned | Visitor owned |
| Allowed in school | ✓ | ✓ | ✓ | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| Full network access | ✓ | ✓ | ✓ | | | |
| Internet only | | | | | ✓* | ✓* |
| No network access | | | | ✓ | | |

* Subject to approval from SLT / Network Manager

# 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
- 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 blog, particularly in association with photographs.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

# Data Protection

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

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

The school must ensure that:

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

- There are clear policies about the use of cloud storage / cloud computing which ensure that such data transfer / storage meets the requirements laid down by the Information Commissioner's Office.
- Where available, staff cloud accounts must be protected with hardware or software based two-factor authentication (2FA).

Staff must ensure that they:

- At all times take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices / services. These are the methods approved by the school for transferring data:
  - internally or externally via Google Workspace applications (Google Docs / Google Drive)
  - externally via a secure file sharing platform (Egress or similar)
  - physically via approved hardware encrypted USB drives

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

- the data must be encrypted and password protected
- USB device access control is implemented and enforced. Data can be saved only on school approved hardware encrypted USB drives. Staff personal USB devices are allowed in 'Read-only' mode.
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

# Communications

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

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

* Designated places: School offices / Meeting rooms / Staff room / off site - away from pupils
** Only the internal messaging system

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

* Designated places: Computer club / Chill-out club

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

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents / carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

# Social Media - Protecting Professional Identity

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

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

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

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

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

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

Monitoring of Public Social Media

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

The school's use of social media for professional purposes will be checked regularly by the senior risk officer and Online Safety Group to ensure compliance with the school policies.

# Unsuitable / inappropriate activities

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

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

**User actions:**

| Acceptable |
| --- |
| • On-line gaming (educational) |
| **Acceptable at certain times** |
| • On-line gaming (non-educational)<br>• On-line shopping / commerce |
| **Acceptable for nominated users** |
| • Use of social media<br>• Use of messaging apps<br>• Use of video broadcasting e.g. Youtube |
| **Unacceptable** |
| • Pornography |

| |
|---|
| • Promotion of any kind of discrimination<br>• Threatening behaviour, including promotion of physical violence or mental harm<br>• 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<br>• Using school systems to run a private business<br>• Unfair usage (downloading / uploading large files that hinders others in their use of the internet) |
| 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:<br>• Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978<br>• Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.<br>• Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008<br>• 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<br>• Promotion of extremism or terrorism<br>• Infringing copyright<br>• Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)<br>• Creating or propagating computer viruses or other harmful files |

# Responding to incidents of misuse

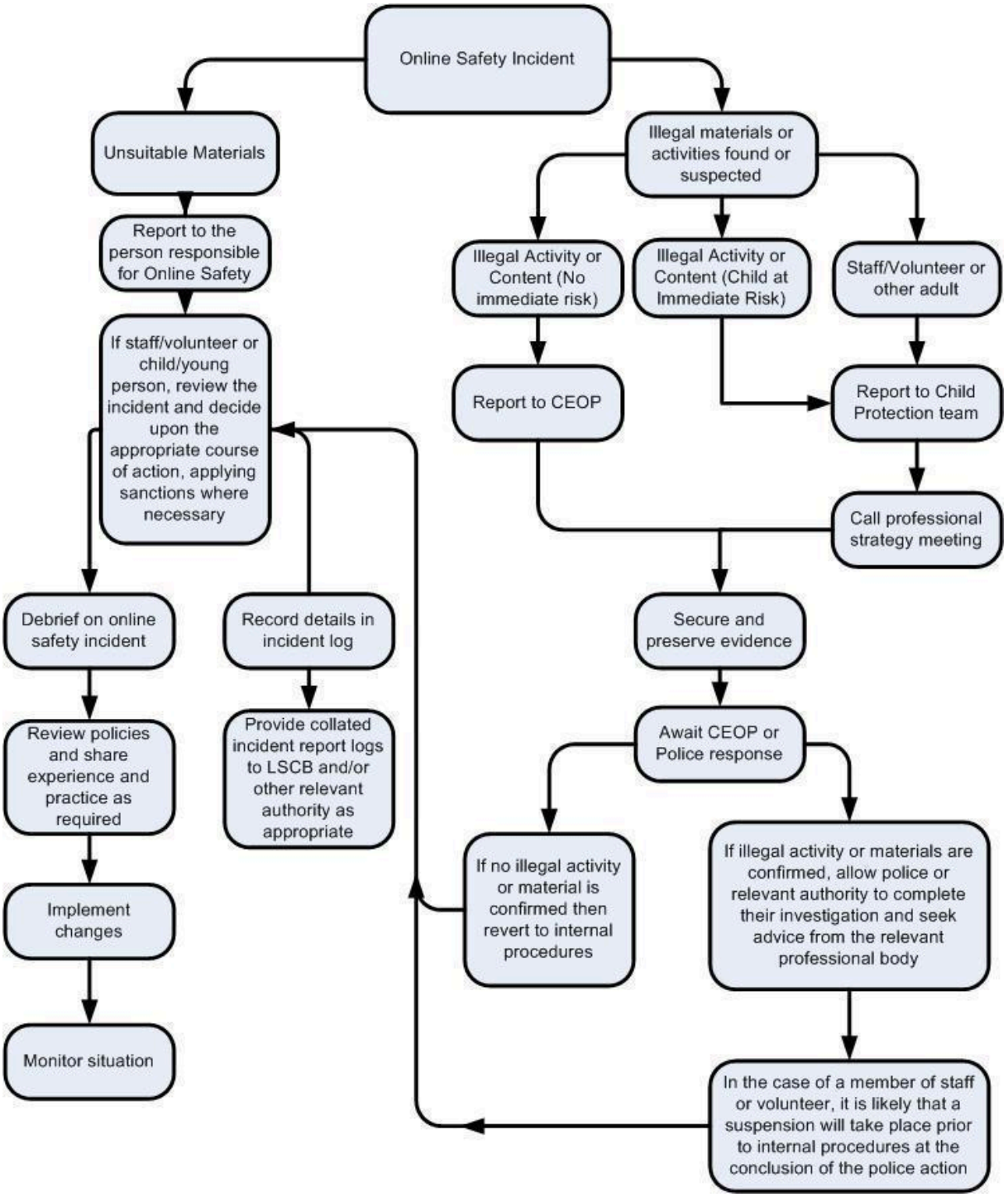
This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

# Reparative

Where pupils misuse equipment within school all incidents will include an element of reparative work whether this be discussions, monitoring or use of external agencies, this will be implemented in partnership with parents/ carers. Reparative work must be carried out before any consequences are put into place, with the exception of serious issues. Please refer to School Actions and Sanctions.

# Illegal Incidents

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



# Other Incidents

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

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

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:

- Internal response or discipline procedures
- Involvement by Local Authority or national / local organisation (as relevant).
- Police involvement and/or action

If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- 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 / disciplinary procedures as follows:

**Pupils:**

| Refer to class teacher / tutor |
| --- |
| • Unauthorised use of non-educational sites during lessons<br>• Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device<br>• Unauthorised / inappropriate use of social media / messaging apps / personal email<br>• Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature |
| Refer to Head of Department / Year / other |
| • Attempting to access or accessing the school network, using the account of a member of staff<br>• Actions which could bring the school into disrepute or breach the integrity of the ethos of the school<br>• Accidentally accessing offensive or pornographic material and failing to report the incident<br>• Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act |

| Refer to Headteacher / Principal |
| --- |
| • Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device<br>• Attempting to access or accessing the school network, using the account of a member of staff<br>• Corrupting or destroying the data of other users<br>• Actions which could bring the school into disrepute or breach the integrity of the ethos of the school<br>• Deliberately accessing or trying to access offensive or pornographic material |
| Refer to Police |
| • Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities). |
| Refer to technical support staff for action re filtering / security etc. |
| • Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).<br>• Unauthorised / inappropriate use of social media / messaging apps / personal email<br>• Unauthorised downloading or uploading of files<br>• Attempting to access or accessing the school network, using the account of a member of staff<br>• Attempting to access or accessing the school network, using another student's / pupil's account<br>• Allowing others to access school network by sharing username and passwords<br>• Corrupting or destroying the data of other users<br>• Using proxy sites or other means to subvert the school's filtering system |
| Inform parents / carers |
| • Attempting to access or accessing the school network, using the account of a member of staff<br>• Attempting to access or accessing the school network, using another student's / pupil's account<br>• Using proxy sites or other means to subvert the school's filtering system<br>• Corrupting or destroying the data of other users |

| |
|---|
| • Deliberately accessing or trying to access offensive or pornographic material |
| **Removal of network / internet access rights** |
| • Attempting to access or accessing the school network, using the account of a member of staff<br>• Attempting to access or accessing the school network, using another student's / pupil's account<br>• Allowing others to access school network by sharing username and passwords<br>• Corrupting or destroying the data of other users<br>• Using proxy sites or other means to subvert the school's filtering system<br>• Deliberately accessing or trying to access offensive or pornographic material |
| **Warning** |
| • Unauthorised downloading or uploading of files |
| **Further sanction eg detention / exclusion** |
| • Continued infringements of the above, following previous warnings or sanctions |

**Staff:**

| Refer to line manager |
| --- |
| • Students / Pupils Incidents<br>• Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).<br>• Unauthorised use of non-educational sites during lessons<br>• Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature<br>• Accidentally accessing offensive or pornographic material and failing to report the incident |
| **Refer to Headteacher** |
| • Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device<br>• Unauthorised / inappropriate use of social media / messaging apps / personal email<br>• Attempting to access or accessing the school network, using the account of a member of staff<br>• Corrupting or destroying the data of other users<br>• Actions which could bring the school into disrepute or breach the integrity of the ethos of the school<br>• Deliberately accessing or trying to access offensive or pornographic material |
| **Refer to Local Authority / HR** |
| • Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature |
| **Refer to Police** |
| • Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities). |
| **Refer to Technical Support Staff for action re filtering etc.** |
| • Pupils Incidents |

| |
|---|
| • Attempting to access or accessing the school network, using another student's / pupil's account<br>• Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).<br>• Attempting to access or accessing the school network, using the account of a member of staff<br>• Corrupting or destroying the data of other users<br>• Using proxy sites or other means to subvert the school's filtering system<br>• Deliberately accessing or trying to access offensive or pornographic material |
| Warning |
| • Unauthorised downloading or uploading of files<br>• Allowing others to access school network by sharing username and passwords<br>• Using proxy sites or other means to subvert the school's filtering system |
| Suspension |
| • Deliberately accessing or trying to access offensive or pornographic material |
| Disciplinary action |
| • Corrupting or destroying the data of other users<br>• Actions which could bring the school into disrepute or breach the integrity of the ethos of the school<br>• Continued infringements of the above, following previous warnings or sanctions |