*This policy was approved by the Full Governing Body on 25 September 2024*

Mill Water School

Preparation for *their* best future

# Online Safety Policy

## and Acceptable Use Policies

September 2024

This policy applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

**Review Date: September 2025**

*This policy was approved by the Full Governing Body on 25 September 2024*

# Content


- **Online Safety Policy**
  - Scope of the Online Safety Policy
  - Policy Development, Monitoring and Review
  - Schedule for Development, Monitoring and Review
  - Monitoring the impact of the Online Safety Policy
- **Policy and Leadership**
  - Responsibilities
  - Online Safety Group
  - Professional Standards
- **Policy**
  - Online Safety Policy
  - Acceptable Use
  - User Actions
  - Reporting and Responding
  - Online Safety Incident Flowchart
  - School Actions
  - Online Safety Education
  - Contribution of Learners
  - Staff / Volunteers
  - Governors
  - Families
- **Technology**
  - Infrastructure and Security
  - Bring your own device (BYOD)
  - Social Media
  - Digital and Video Images
  - Online Publishing
  - Data Protection
- **Outcomes**
- **Appendices**
  - Mill Water School Filtering Policy
  - Mill Water School Password Security Policy
  - 14 Rules for Responsible ICT Use
  - Acceptable Use Policy for Pupils
  - Acceptable Use Policy for Parents/Carers
  - Acceptable Use Policy for Staff and Volunteers
  - Email Policy and Code of Practice
  - Use of Digital Images – Pupils (+ consent form)
  - Use of Digital Images – Staff (+ consent form)
  - Legislation

*This policy was approved by the Full Governing Body on 25 September 2024*

# Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of Mill Water School to safeguard members of our school community online in accordance with statutory guidance and best practice. Mill Water School is aware of the legislative framework under which this Online Safety Policy template and guidance has been produced as outlined in the attached 'Legislation' Appendix.

This Online Safety Policy applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Mill Water 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.

# Policy Development, Monitoring and Review

This Online Safety Policy has been developed by the Mill Water School Online Safety Group, made up of:

- Online Safety Lead
- Staff – including teachers/support staff/technical staff
- Governor

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

# Schedule for Development, Monitoring and Review

| | |
|---|---|
| The Mill Water Online Safety Policy was approved by the Governing Body on: | September 2024 |
| The implementation of this Online Safety Policy will be monitored by the: | Online Safety Lead, IT Manager, School Business Manager, Headteacher |
| Monitoring will take place at regular intervals: | Annually or as required |
| The Governing Body will receive a report on the implementation of the Online Safety Policy generated by the Online Safety Working Group (which will include anonymous details of online safety incidents) at regular intervals: | Annually or as required |
| The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be: | September 2025 |
| Should serious online safety incidents take place, the following external persons/agencies should be informed: | CEOP, The Police, LADO, Children's Services |

*This policy was approved by the Full Governing Body on 25 September 2024*

## Monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using:

- Logs of reported incidents (via Safeguarding Termly Report to Governors)
- SWGfL (Southwest Grid for Learning) monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys / Questionnaires of:
    - Learners – through the school council
    - Parents and carers - through the Headteacher's annual parent survey
    - Staff – through the National Online Safety Hub, training / discussion

# Policy and Leadership

## Responsibilities

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

### Headteacher and senior leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety may be delegated to the Online Safety Lead.
- The Headteacher and DSL 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.
- The Headteacher is responsible for ensuring that the Online Safety Lead, technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and 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.
- The Headteacher will receive regular monitoring reports from the Online Safety Lead.

### Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This review will be carried out by the Safeguarding Governor who will also take on the role of Online Safety Governor. They will receive regular information about online safety incidents and monitoring reports.

*This policy was approved by the Full Governing Body on 25 September 2024*

The Safeguarding/Online Safety Governor will:

- have regular meetings with the Online Safety Lead
- receive (collated and anonymised) reports of online safety incidents
- check that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training are taking place as intended).
- report back to Full Governing Body

The Governing Body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

## Online Safety Lead

The Online Safety Lead will:

- lead the Online Safety Group
- take day-to-day responsibility for online safety issues, being aware of the potential for serious child protection concerns
- have a leading role in establishing and reviewing the school online safety policies/documents
- promote an awareness of and commitment to online safety education / awareness raising across the school and beyond
- liaise with curriculum lead to ensure that the online safety curriculum is planned, mapped, embedded, and evaluated
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- receive reports of online safety incidents and create a log of incidents to inform future online safety developments
- provide (or identify sources of) training and advice for staff/governors/parents/carers/learners
- liaise with school/local authority technical staff, pastoral staff and support staff (as relevant)
- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and if possible, filtering and monitoring logs
- attend relevant governing body meetings
- report regularly to Headteacher
- liaise with the local authority.

## Designated Safeguarding Lead (DSL)

The Designated Safeguarding Lead is trained in online safety issues and is aware of the potential for serious 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
- online bullying.

## Curriculum Lead

Curriculum Lead will work with the Online Safety Lead to develop a planned and coordinated online safety education programme.

This will be provided through:

- a discrete programme
- PHSE and RSHE programmes
- a mapped cross-curricular programme
- assemblies and pastoral programmes
- relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

## Teaching and support staff

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood, and signed the staff acceptable use agreement (AUA)
- they immediately report any suspected misuse or problem to SLT for investigation/action, in line with the school safeguarding procedures
- all digital communications with learners and 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
- ensure learners, where they are able, understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- in lessons where internet use is pre-planned learners 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 lessons take place using live-streaming or video-conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies and should take note of the guidance contained in the SWGfL Safe Remote Learning Resource
- have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

## IT Manager

The IT Manager is responsible for ensuring that:

- they are aware of and follow the school Online Safety Policy and Technical Security Policy to carry out their work effectively in line with school policy
- the school technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets (as a minimum) the required online safety technical requirements as identified by the local authority
- there is clear, safe, and managed control of user access to networks and devices
- 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
- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the Headteacher for investigation and action
- the filtering policy is applied and updated on a regular basis.

## Learners

- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy, which includes personal devices such as iPads used as AAC devices
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should know what to do if they or someone they know feels vulnerable when using online technology
- 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 and carers

The school will take every opportunity to help parents and carers understand these issues through:

- publishing the school Online Safety Policy on the school website
- providing them with a copy of the learners' acceptable use agreement and asking them to sign
- publishing information about appropriate use of social media relating to posts concerning the school
- seeking their permissions concerning use of digital images, use of apps such as Evidence for Learning
- parents'/carers' meetings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Parents and carers will be encouraged to support the school in:

- reinforcing the online safety messages provided to learners in school
- the use of their children's personal devices in the school (where this is allowed).

*This policy was approved by the Full Governing Body on 25 September 2024*

## Online Safety Group

The Online Safety Group has the following members:

- Online Safety Lead/DSL
- School Business Manager
- Online Safety Governor
- IT Manager
- Teacher/curriculum lead

Members of the Online Safety Group will assist the Online Safety Lead 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 education provision – ensuring relevance, breadth, progression, and coverage
- reviewing network/filtering/monitoring/incident logs, where possible
- encouraging the contribution of learners to staff awareness, emerging trends, and the school online safety provision
- consulting stakeholders, including staff/parents/carers, about the online safety provision
- monitoring improvement actions identified through use of the NOS audit tool.

## Professional Standards

There is an expectation that required professional standards will be applied to online safety as in other aspects of school life i.e., policies and protocols are in place for the use of online communication technology between the staff and other members of the school and wider community, using officially sanctioned school mechanisms.

# Policy

## Online Safety Policy

The school Online Safety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- allocates responsibilities for the delivery of the policy
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world

- describes how the school will help prepare learners to be safe and responsible users of online technologies
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- is supplemented by a series of related acceptable use agreements
- is made available to staff at induction
- is published on the school website.

# Acceptable Use

The school has defined what it regards as acceptable/unacceptable use and this is shown in the tables below.

### Acceptable use agreements

The Online Safety Policy and acceptable use agreements define acceptable use at the school. The acceptable use agreements will be communicated/re-enforced through:

- pre-employment meetings with School Business Manager
- staff induction and staff handbook
- posters in classrooms
- communication with parents/carers
- through regular IT/online safety/PSHE/RSHE sessions
- school website.

| User Actions | | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
|---|---|---|---|---|---|---|
| Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to: | **Any illegal activity for example:**<br>• Child sexual abuse imagery*<br>• Child sexual abuse/exploitation/grooming<br>• Terrorism<br>• Encouraging or assisting suicide<br>• Offences relating to sexual images i.e., revenge and extreme pornography<br>• Incitement to and threats of violence<br>• Hate crime<br>• Public order offences - harassment and stalking<br>• Drug-related offences<br>• Weapons / firearms offences<br>• Fraud and financial crime including money laundering<br>**Responding to and managing sexting incidents**<br>**Sexting in schools and colleges** | | | | | ✓ |

| | | | | | | |
|---|---|---|---|---|---|---|
| Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990) | • Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised)<br>• Gaining unauthorised access to school networks, data and files, through the use of computers/devices<br>• Creating or propagating computer viruses or other harmful files<br>• Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords)<br>• Disable/Impair/Disrupt network functionality through the use of computers/devices<br>• Using penetration testing equipment (without relevant permission)<br><br>Serious or repeat offences will be reported to the police. Under the Cyber-Prevent agenda the National Crime Agency has a remit to prevent learners becoming involved in cyber-crime and harness their activity in positive ways – further information **here** | | | | | ✓ |
| Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies: | Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs) | | | | ✓ | |
| | Promotion of any kind of discrimination | | | | ✓ | |
| | Using school systems to run a private business | | | | ✓ | |
| | Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school | | | | ✓ | |
| | Infringing copyright | | | | | ✓ |
| | Unfair usage (downloading/uploading large files that hinders others in their use of the internet) | | | | ✓ | |
| | 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 | | | | ✓ | |

| Consideration should be given for the following activities when undertaken for non-educational purposes: | Staff & other adults | | | | Pupils | | | |
|---|---|---|---|---|---|---|---|---|
| | Allowed | Allowed at certain times | Allowed for selected staff | Not allowed | Allowed | Allowed at certain times | Allowed with staff permission | Not allowed |
| On-line gaming | | ✓ | | | | | | ✓ |
| Online shopping/commerce | | ✓ | | | | | | ✓ |
| File sharing | | | | ✓ | | | | ✓ |
| Social Media | | ✓ | | | | | | ✓ |
| Messaging/chat | | ✓ | | | | | | ✓ |
| Entertainment streaming e.g. Netflix, Disney+ | | ✓ | | | | | | ✓ |
| Use of video broadcasting, e.g. YouTube, Twitch, TikTok | | | ✓ | | | | | ✓ |
| Mobile phones may be brought to school | ✓ | | | | | | ✓ | |
| Use of personal mobile phones for learning at school | | | | ✓ | | | | ✓ |
| Use of personal mobile phones in social time (in staff room or off site) | ✓ | | | | | | | ✓ |
| Taking photos on personal mobile phones or other devices | | | | ✓ | | | | ✓ |
| Use of other personal mobile devices eg tablets, gaming devices | ✓ | | | | | | ✓ | |
| Use of personal email in school, or on school network/wifi | | | | ✓ | | | | ✓ |
| Use of school email for personal emails | | | | ✓ | | | | ✓ |

*This policy was approved by the Full Governing Body on 25 September 2024*

When using communication technologies, Mill Water School considers the following as good practice:

- when communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school
- any digital communication between staff and learners or parents/carers (e-mail, social media, etc.) must be professional in tone and content. Personal e-mail addresses, text messaging or social media must not be used for these communications.
- staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community
- users should immediately report to a 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
- relevant policies and permissions should be followed when posting information online e.g., school website and social media.
- a growing number of pupils are using personal iPads as communication devices (AAC device)

# Reporting and Responding

Mill Water School will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention.

The school will ensure:

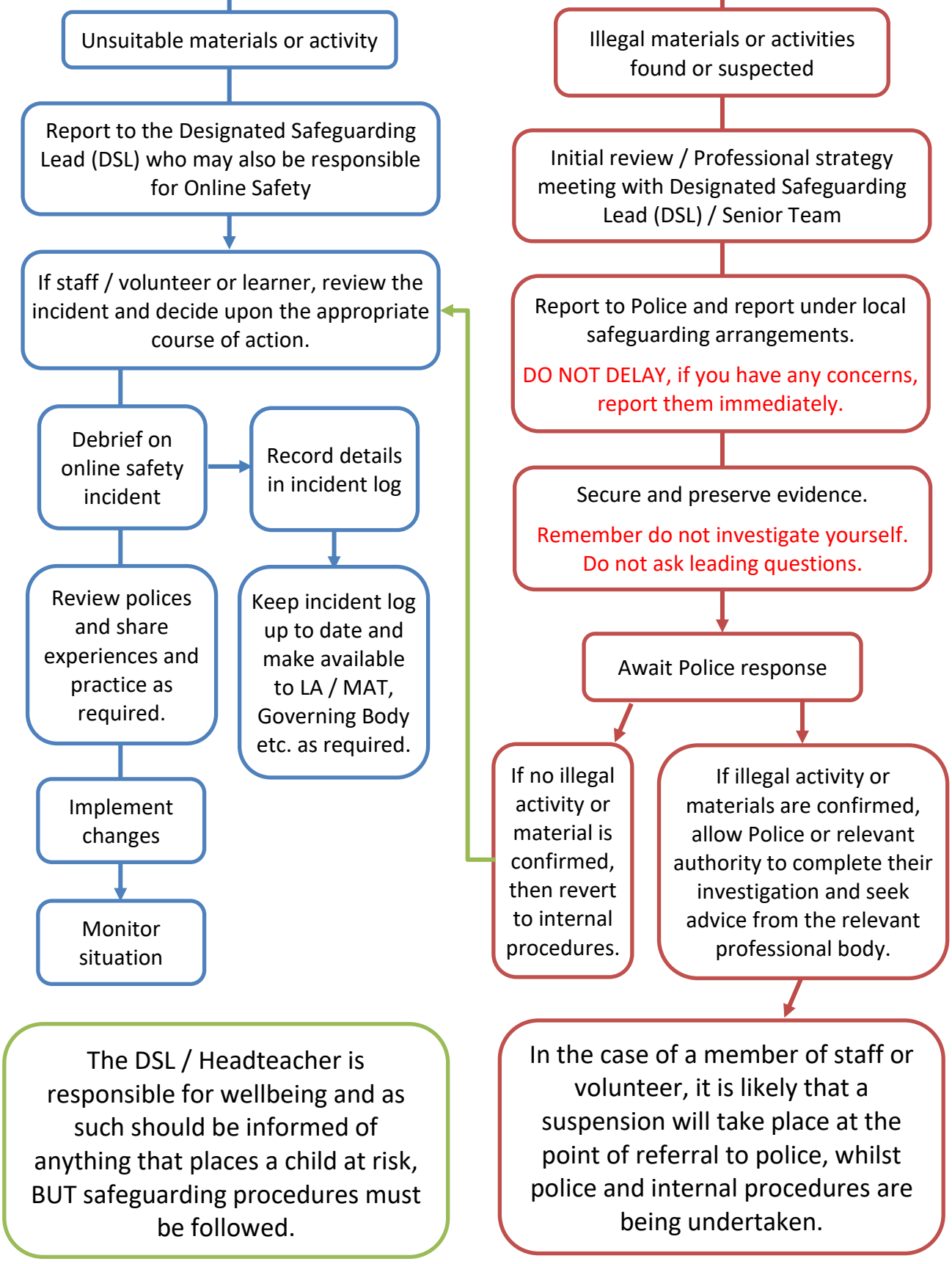
- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies
- all members of the school community will be made aware of the need to report online safety issues/incidents
- reports will be dealt with as soon as is possible once they are received
- the Designated Safeguarding Lead/Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm (see flowchart on page 14), the incident must be escalated through the agreed school safeguarding procedures
- any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the local authority designated officer (LADO)
- where there is no suspected illegal activity, devices may be checked using the following procedures:
    - one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.

  - conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
  - ensure that the relevant staff 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.
  - 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
    - police involvement and/or action

- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
- incidents should be logged on CPOMS if the incident involves a learner.
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; **Professionals Online Safety Helpline**; **Reporting Harmful Content**; **CEOP**.
- where appropriate, those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions.
- learning from the incident (or pattern of incidents) will be provided to:
  - the Online Safety Group for consideration of updates to policies or curriculum programmes and to review how effectively the report was dealt with
  - staff, through regular briefings
  - learners, through assemblies/lessons
  - parents/carers, through newsletters, school social media, website
- governors, through regular safeguarding updates
- local authority/external agencies, as relevant.

The school will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.

# Online Safety Incident Flowchart




The DSL / Headteacher is responsible for wellbeing and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.

In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

# School Actions

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:

| **Responding to Learner Actions** | **Actions / Sanctions** | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Incidents:<br>Each incident will be discussed, investigated and proportionate action taken | Refer to class teacher | Refer to Headteacher | Refer to Police | Refer to tech support staff for action | Inform parents / carers | Removal of network / internet access rights | Education/Warning | Further sanction eg exclusion |
| Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities). | | ✓ | | | ✓ | | ✓ | |
| Attempting to access or accessing the school network, using another user's account (staff or learner) or allowing others to access school network by sharing username and passwords | ✓ | | | | ✓ | | ✓ | |
| Corrupting or destroying the data of other users | ✓ | | | | ✓ | | ✓ | |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | | ✓ | | | ✓ | | ✓ | |
| Unauthorised downloading or uploading of files | ✓ | | | | ✓ | | ✓ | |
| Using proxy sites or other means to subvert the school's filtering system | ✓ | | | | ✓ | | ✓ | |
| Accidentally accessing offensive or pornographic material and failing to report the incident | | ✓ | | | ✓ | | ✓ | |
| Deliberately accessing or trying to access offensive or pornographic material | | ✓ | | | ✓ | | ✓ | |
| Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act | ✓ | | | | ✓ | | ✓ | |
| Unauthorised use of digital devices (including taking images) | ✓ | | | | ✓ | | ✓ | |
| Unauthorised use of online services | | ✓ | | | ✓ | | ✓ | |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school | | ✓ | | | ✓ | | ✓ | |
| Continued infringements of the above, following previous warnings or sanctions | | | | | ✓ | | ✓ | ✓ |

| Responding to staff actions | Actions / Sanctions | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Incidents: | Refer to line manager | Refer to Headteacher | Refer to Local Authority / HR | Refer to Police | Refer to Tech Support Staff for action | 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). | | ✓ | ✓ | ✓ | | | ✓ | ✓ |
| Deliberate actions to breach data protection or network security rules | | ✓ | ✓ | | | | ✓ | |
| Deliberately accessing or trying to access offensive or pornographic material | | ✓ | ✓ | ✓ | | | ✓ | ✓ |
| Corrupting or destroying the data of other users or causing deliberate damage to hardware or software | | ✓ | | | | | ✓ | ✓ |
| Using proxy sites or other means to subvert the school's filtering system | | ✓ | | | | | ✓ | ✓ |
| Unauthorised downloading or uploading of files or file sharing | | ✓ | | | | | | |
| Breaching copyright or licensing regulations | | ✓ | | | | | | |
| 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 | | ✓ | | | | | | |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | | ✓ | | | | | | ✓ |
| Using personal email/social networking/messaging to carry out digital communications with pupils or parents/carers | | ✓ | | | | | | |
| Inappropriate personal use of digital technologies ie social media/ personal email | | ✓ | | | | | | ✓ |
| Careless use of personal data eg displaying, holding or transferring data in an insecure manner | | ✓ | | | | | | |
| Actions which could compromise the staff member's professional standing | | ✓ | | | | | | |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school | | ✓ | | | | | | ✓ |
| Failing to report incidents whether caused by deliberate or accidental actions | | ✓ | | | | ✓ | | |
| Continued infringements of the above, following previous warnings or sanctions | | ✓ | | | | | | ✓ |

# Online Safety Education Programme

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:

- an online safety curriculum, adapted to meet the needs of our pupils, matched against Education for a Connected World Framework by UKCIS/DCMS and regularly taught in a variety of contexts.
- sessions are matched to need; are age/stage appropriate and build on prior learning
- sessions are context-relevant with agreed objectives leading to clear and evidenced outcomes
- learner need and progress are addressed through effective planning and assessment
- digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; RSHE; Literacy etc
- it incorporates, where appropriate, relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- where appropriate, learners should be helped to understand the need for the learner 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 learners 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 learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites they visit
- the online safety curriculum should be relevant and up to date to ensure the quality of learning and outcomes.

# Contribution of Learners

Mill Water School acknowledges the contribution that learners can make. Their contribution is recognised through:

- pupil feedback from the School Council.
- learners contribute to the online safety programme e.g. peer education, online safety campaigns
- contributing to online safety events with the wider school community e.g. parents' evenings

# Staff / Volunteers

All staff will receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- formal online safety and data protection training will be made available to all staff. Staff will have access to the National Online Safety Hub and will be directed to undertake specific training sessions as part of a regular refreshers. An audit of the online safety training needs of all staff will be carried out regularly.
- the training will be an integral part of the school's annual safeguarding and data protection training for all staff
- all new staff will 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 includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours
- the Online Safety Lead/ Designated Safeguarding Lead (or other nominated person) will receive regular updates through attendance at external training events, (e.g. UKSIC / 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
- the Online Safety Lead (or other nominated person) will provide advice/guidance/training to individuals as required.

# Governors

**Governors should take part in online safety training/awareness sessions**, with particular importance for those who are involved in technology/online safety/health and safety/safeguarding. This may be offered in several ways such as:

- attendance at training provided by the local authority or other relevant organisation (e.g. SWGfL)
- participation in school training / information sessions for staff or parents

A higher level of training will be made available to the Online Safety Governor.

# Families

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

- regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes. Parents/carers receive regular newsletters which include a link to the National Online Safety Hub topic of the week. Parents are invited to register as users on the NOS hub
- regular opportunities for engagement with parents/carers on online safety issues through awareness workshops / parent/carer meetings
- the learners, who are encouraged to pass on to parents the online safety messages they have learned in school
- School website
- high profile events / campaigns e.g. Safer Internet Day
- reference to the relevant web sites/publications, e.g. SWGfL; saferinternet; childnet
- Sharing good practice with other schools within the Exmouth Learning Community, SENtient Trust, or during local authority training sessions.

# Technology

## Infrastructure and Security

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

- School IT systems will be managed in ways that ensure that the school meets the online safety technical requirements outlined in the SWGfL Technical Security Policy and Acceptable Use Policy and any relevant Local Authority Online Safety Policy and guidance.
- There will be regular reviews and audits of the safety and security of school IT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school IT systems. Details of the access rights available to groups of users will be recorded by the IT Manager and will be reviewed, at least annually, by the Online Safety Working Group.
- All users, for whom it is appropriate, will be provided with a username and password by the IT Manager who will keep an up to date record of users and their usernames. User passwords will be changed on advice from the IT Manager.
- The "administrator" passwords for the school IT system, used by the IT Manager, must also be available to the Headteacher or School Business Manager and kept securely by the School Business Manager.
- The IT 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.
- 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.
- Internet access is filtered for all users.
- Internet filtering ensures that children are safe from terrorist and extremist material when accessing the internet.
- The school maintains and supports the managed filtering service provided by SWGfL.
- In the event of the IT Manager needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher (or other nominated senior leader).
- Any filtering issues should be reported immediately to SWGfL.
- Requests from staff for sites to be removed from the filtered list will be considered by the Online Safety Coordinator and Headteacher. If the request is agreed, this action will be recorded, and logs of such actions shall be reviewed regularly by the Online Safety Working Group.
- School IT Manager regularly monitors and records the activity of users on the school IT systems and users are made aware of this in the Acceptable Use Policy
- Any IT incident will be emailed to IT Manager.

- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, visitors) onto the school system. Any visitors who need access to the school system will be given temporary log in details by the IT Manager. These details will be personalised and removed when no longer required.
- The downloading of executable files is managed by the IT Manager.
- School devices are not for personal use and are used in accordance with our Data Protection Policy.
- An agreed policy is in place regarding the use of removable media (eg memory sticks/CDs/DVDs) by users on school systems/portable devices.
- The school infrastructure and individual workstations are protected by up-to-date virus software.
- Personal data is not sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

# Bring your own device (BYOD)

As a rule, children can bring their own devices into school but will hand them in to reception on arrival at school where they will be kept safe until home time. This is likely to be iPods, iPads etc for use on school transport.

A growing number of children bring in their own tablets or iPads (AAC devices) which are used specifically to support communication and form part of a plan developed in conjunction with the class teacher, speech and language staff and parents /carers.

All equipment used in school is subject to the Online Safety Policy and relevant AUP and has been passed to the IT Manager prior to use in the classroom. Filtering settings and restrictions are applied to the device by the IT Manager. All devices in school are subject to the same level of filtering, monitoring, and restrictions as school devices.

Pupils' devices used in school are used only for specific purposes outlined in their speech and language programme. These devices are used under the supervision of classroom adults who are responsible for safeguarding other pupils against unauthorised photography or videoing.

Authorised programmes currently used at Mill Water consist of Proloquo2go and Grid Player.

# Social Media

All schools have a duty of care to provide a safe learning environment for pupils and staff. Schools could be held responsible, indirectly, for acts of their employees in the course of their employment. Staff members who harass, bully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school liable to the injured party.

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

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

School staff should ensure that:

- No reference should be made on personal social media to pupils, parents/carers or school staff
- Their friends are not parents of pupils attending Mill Water School, or pupils
- No pictures of pupils attending Mill Water School are posted on personal social media sites
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information or unwanted access

## School Use of Social Media

The school currently uses Facebook and Instagram for connecting with parents and carers, the local community and former pupils in order to:

- enhance our communication, which already includes use of the school website, home school books, email, newsletters, telephone calls, zoom/teams meetings
- increase awareness about the school in the local community
- facilitate communication and networking opportunities between parents, especially new or prospective parents
- publicise the school calendar and fundraising events
- maintain contact with former pupils and parents
- announce any new information as it appears on the school website
- highlight school achievements in a forum where they can be shared by the school community
- showcase the broad range of curriculum activities provided to our pupils.

We follow the guidelines below:

- The school Facebook Page and Instagram Profile is password protected and can only be updated by named members of staff.
- The Headteacher will approve all draft updates before they are published.
- Where possible, utilising the built-in tools, comments, tags or sharing content is prevented.
- The Facebook Page and Instagram Profile is monitored regularly to ensure compliance and accuracy.

Important: Facebook has a minimum age requirement of 13. All parents are reminded that children under the age of 13 should not be on Facebook

The school's use of social media for professional purposes will be checked regularly by the Online Safety Working Group to ensure compliance with the Data Protection, Communications and Digital Image and Video Policies.

### Personal Use of Social Media

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

### Monitoring of Social Media

- As part of active social media engagement, the school may pro-actively monitor the Internet for public postings about the school
- the school should effectively respond to social media comments made by others according to a defined policy or process
- when parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.

## Digital and Video Images

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- the school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies.
- when using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images.
- staff/volunteers must be aware of those learners whose images must not be taken/published. Those images should only be taken on school devices. The personal devices of staff should not be used for such purposes.
- in accordance with guidance from the Information Commissioner's Office, parents/carers can 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 learners 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, storage, distribution and publication of those images
- care should be taken when sharing digital/video images that learners are appropriately dressed
- learners must not take, use, share, publish or distribute images of others without their permission
- photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with Online Safety Policy

- learners' full names will not be used anywhere on a website or blog, particularly in association with photographs
- written permission from parents or carers will be obtained before photographs of learners are taken for use in school or published on the school website/social media.
- parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy
- images will be securely stored in line with the school retention policy
- learners' work can only be published with the permission of the learner and parents/carers.

# Online Publishing

The school communicates with parents/carers and the wider community and promotes the school through:

- Public-facing website
- Social media
- Online newsletters

The school website is managed by the school's IT Manager. The school ensures that online safety policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of learners, publication of school calendars and personal information – ensuring that there is least risk to members of the school community, through such publications.

Where learner work, images or videos are published, their identities are protected, and full names are not published.

The school public online publishing provides information about online safety e.g., publishing the school's Online Safety Policy and acceptable use agreements; curating latest advice and guidance; news articles etc, making reference to the National Online Safety Hub, creating an online safety page on the school website.

# Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation. It will 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.

Refer to our **Data Protection Policy and Privacy Notices on our school website** for more information.

# Outcomes

The impact of the Online Safety Policy and practice is regularly evaluated through the review of online safety incident logs; behaviour/bullying reports; surveys of staff, learners; parents/carers and is reported to relevant groups:

- there is balanced professional debate about the evidence taken from the reviews and the impact of preventative work e.g., online safety education, awareness, and training
- there are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and Governors
- parents/carers are informed of patterns of online safety incidents as part of the school's online safety awareness raising
- online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate
- the evidence of impact is shared with other schools, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.

# Appendices

## Mill Water School Filtering Policy

### 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. It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

As a part of the South West Grid for Learning (SWGfL), schools and connected organisations automatically receive the benefits of a managed filtering service, with some flexibility for changes at local level.

### Responsibilities

The responsibility for the management of the school's filtering policy will be held by the Online Safety Coordinator. 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 SWGfL / school filtering service that involve allowing a previously filtered site must:

- be logged and be reported to the Headteacher
- be reported to the Online Safety Governor annually

All users have a responsibility to report immediately to the Online Safety Coordinator 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.

### Education / Training / Awareness

Pupils will be made aware of the importance of filtering systems through the online safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- signing the AUP
- induction training
- staff meetings, briefings, Inset.

*This policy was approved by the Full Governing Body on 25 September 2024*

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

## Changes to the Filtering System

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the Online Safety Coordinator who will decide whether to make school level changes. If it is felt that the site should be filtered (or unfiltered) at SWGfL level, the Online Safety Coordinator should email **filtering@swgfl.org.uk** with the URL.

## Audit / Reporting

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

- Headteacher
- Online Safety Governor

The filtering policy will be reviewed in response to the evidence provided by the audit logs of the suitability of the current provision.

*This policy was approved by the Full Governing Body on 25 September 2024*

# Mill Water School Password Security Policy

## Introduction

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access.
- no user should be able to access another's files, without permission (or as allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the school's Data Protection Policy.
- logs are maintained of access by users and of their actions while users of the system.

A safe and secure username / password system is essential if the above is to be established and will apply to all school IT systems, including email.

## Responsibilities

The management of the password security policy will be the responsibility of the IT Manager.

All users, other than those with group logons, will have responsibility for the security of their username and password and 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 the IT Manager.

## Training / Awareness

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

- at induction
- through the school's Online Safety Policy and Password Security Policy
- through the Acceptable Use Agreement.

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

- in ICT and online safety lessons
- through the Acceptable Use Agreement.

## Policy Statements

All users will have clearly defined access rights to school IT systems. Details of the access rights available to groups of users will be recorded by the IT Manager and will be reviewed, at least annually, by the Online Safety Working Group.

All adult users will be provided with a username and password by the IT Manager who will keep an up to date record of users and their usernames.

Some individual pupils will be allocated their own username and password. This will be determined by the Online Safety Coordinator. All other pupils will use a group log-on which will not be changed.

The following rules apply to the use of passwords:

- Pupils with their own log-ins will be provided with simple passwords that cannot be changed
- All other users will be required to use more complex passwords; the level of complexity will be determined by the level of access the user has to IT systems – an on screen message will be displayed if a user is required to provide a more complex password during a password change/reset
- Users with access to sensitive, personal or financial data will be required to change their passwords regularly (managed by IT Manager)
- User accounts should be "locked out" when the number of incorrect log-on attempts is exceeded (pupils=0, staff=5, guests=3)
- Passwords will not be displayed on screen, and will be securely hashed
- Users will be alerted by the IT Manager in person or via an on screen message when a password change/reset is required. The IT Manager will manage and log all requests for password changes and support users who need to reset a forgotten password.
- The "administrator" password for the school IT system, used by the IT Manager must also be available to the Headteacher and School Business Manager and kept in the school safe.

## Audit / Monitoring / Reporting / Review

The IT Manager will ensure that full records are kept of:

- User IDs and requests for password changes
- User logons
- Security incidents related to this policy

In the event of a serious security incident, the police may request and will be allowed access to passwords used for encryption.

Local Authority Auditors also have the right of access to passwords for audit investigation purposes.

User lists, IDs and other security related information must be given the highest security classification and stored in a secure manner.

These records will be reviewed by the Online Safety Working Group and Online Safety Governor annually.

This policy will be reviewed annually in response to changes in guidance and evidence gained from the logs.

Mill Water School

Preparation for *their* best future

# 14 Rules for Responsible ICT Use

**These rules will keep everyone safe and help us to be fair to others.**

1. I will only use the school's laptops and iPads for schoolwork or with permission.
2. I will only delete my own files.
3. I will not look at other people's files without their permission.
4. I will keep my login and password secret.
5. I will not bring CDs, memory sticks or other devices into school without permission.
6. If I bring my mobile phone to school, I will hand it in at reception or keep it in a safe place and will not use it during the school day without permission.
7. I will ask permission from a member of staff before using the internet.
8. When I am at school I will only use the school email.
9. I will only e-mail people I know, or my teacher has approved.
10. The messages I send, or information I upload, will always be polite and sensible.
11. I will not open an attachment or download a file unless I have permission or I know and trust the person who has sent it.
12. I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless my teacher has given permission.
13. I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room.
14. If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will tell a teacher/responsible adult.

*This policy was approved by the Full Governing Body on 25 September 2024*

Mill Water School

Preparation for *their* best future

# Acceptable Use Policy for Pupils

## Keeping Safe: Stop, Think, before you Click!

Pupil name:.....

These rules will keep everyone safe and help us to be fair to others.

1. I will only use the school's laptops and iPads for schoolwork or with permission.
2. I will only delete my own files.
3. I will not look at other people's files without their permission.
4. I will keep my login and password secret.
5. I will not bring CDs, memory sticks or other devices into school without permission.
6. If I bring my mobile phone to school, I will hand it in at reception or keep it in a safe place and will not use it during the school day without permission.
7. I will ask permission from a member of staff before using the internet.
8. When I am at school I will only use the school email.
9. I will only e-mail people I know, or my teacher has approved.
10. The messages I send, or information I upload, will always be polite and sensible.
11. I will not open an attachment or download a file unless I have permission or I know and trust the person who has sent it.
12. I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless my teacher has given permission.
13. I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room.
14. If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will tell a teacher/responsible adult.

- ✓ I have read the school '14 rules for responsible IT use'. My teacher has explained them to me.
- ✓ I understand these rules are there to help keep me safe, and my friends and family safe. I agree to follow the rules.
- ✓ This means I will use the school computers, laptops, internet, e-mail, digital cameras, video recorders and any other equipment in a safe and responsible way.
- ✓ I understand that the school can check my folders on the school network and the internet sites I visit and that if they have concerns about my safety, they may contact my parent/carer.
- ✓ I understand that if staff still have concerns about my safety, I might not be able to use the computers / laptops anymore.

Pupil's signature:..... Date:.....

*This policy was approved by the Full Governing Body on 25 September 2024*

Mill Water School

Preparation for *their* best future

# Acceptable Use Policy for Parents/Carers

This Acceptable Use Policy is intended to ensure:

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

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

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

## Permission Form

Parents / Carers name:..... Pupil name:.....

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

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

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

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

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Signature:..... Date:.....

*This policy was approved by the Full Governing Body on 25 September 2024*

Mill Water School

Preparation for *their* best future

# Acceptable Use Policy for Staff, Governors and Volunteers

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school IT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of IT in their everyday work.
- that the school is compliant with its duty under the General Data Protection Regulations (GDPR).

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

## Acceptable Use Policy Agreement

I understand that I must use school IT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the IT systems and other users. I recognise the value of the use of IT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of IT. I will, where possible, educate the young people in my care in the safe use of IT 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 school digital technology and communication systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (eg laptops, email, SIMS, RM Unify etc) out of school, and to the transfer of personal data (digital or paper based) out of school (see Data Protection Policy 2020).
- I understand that the school digital technology systems are intended for educational use and professional use and that therefore, I will not hold non-work related data on the school IT systems. Where I have access to any portable systems (laptop/tablet) I will not permit any unauthorised access to this device.
- 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 my password should be kept securely and will be managed by the IT Manager.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the IT Manager or a Senior Leader.

I will be professional in my communications and actions when using school IT 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. Where these images are published (eg. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.

- I will not use chat and social networking sites in school time. I will only use social networking sites in school in accordance with the school's policy (See Online Safety Policy).
- I will only communicate with parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities.

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

- When I use my mobile devices (laptops/tablets/mobile phones /USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school 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 register my school email address to conduct personal business (such as Ebay)
- I will not open any hyperlinks in emails or 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 be responsible for backing up data on any external devices I use.
- 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 authorised.
- 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 Mill Water School Data Protection Policy. Where digital personal data is transferred outside the secure school network, it must be encrypted, password protected or sent via Egress. I understand that this also applies to any data I download/store on any device, in order that the data cannot be accessed should the device get lost or stolen. Paper based Protected and Restricted data must be held in lockable storage – this also applies to material that identifies an individual which is stored on other media ie recordings of school productions, exam material.
- I understand that the Mill Water 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, to the IT Manager.

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 school:

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

**I have read, understood and agree with the Staff and Volunteer Acceptable Use Policy and agree to report any breach of this or other GDPR related policies to the appropriate responsible member of staff - usually the DPO.**

Signed …….. Name …….. Date……..

*This policy was approved by the Full Governing Body on 25 September 2024*

Mill Water School

Preparation for *their* best future

# Email Policy and Code of Practice

## Introduction

In the light of GDPR, it is essential that a written policy and code of practice exists, which sets of the rules and principles for use of email by all. This policy sits alongside our Data Protection Policy and Online Safety Policy, as well as the Acceptable Use Policy which all staff and volunteers are expected to sign and adhere to.

Email has replaced telephone calls and letters in many instances, however the language used in an email is often less formal and more open to misinterpretation than a written memo or formal letter. It is also important to remember that emails are:

- Not always a secure medium – confidential or sensitive information should be sent via a password protected document, with the password contained in a separate email, or by Egress, or by using the built in encryption/protection provision of Office 365. Never put sensitive information in the subject line of an email.
- Subject to disclosure under the access to information regimes – Freedom of Information and Data Protection legislation. Be aware the content of an email could potentially be made public.
- Not necessarily deleted immediately – even if you delete your copy, the recipient may not and these may be subject to disclosure under the access to information regimes.
- Can form a contractual agreement – do not enter into any agreement unless authorised to do so
- Not the place to "store" documentation – attachments should be saved into an appropriate electronic filing system or printed and placed within paper files.
- Monitored by the school.

## Policy

- The School's email system should only be used professionally to conduct School related business. It should not be used for personal use.
- The school email system has a disclaimer automatically applied to all outgoing email. You must not attempt to amend or remove it.
- Do not send personal or sensitive information within an email, unless via Egress, or using the built in encryption/protection provision of Office 365. If you are not using Egress or Office 365 Protection, information should be sent as a password protected document, with the password sent in a separate email.
- Do not open any hyperlinks, attachments or emails unless the source is known and trusted, due to the risk of viruses and other harmful programmes. If you have any concerns over the validity of an email, contact the IT Manager.
- A retention label is applied to all school emails displaying an expiry date when the email will be permanently deleted from the mailbox. You are advised to regularly delete material you no longer require and archive material that you wish to keep. Please contact the IT Manager if you need help with this.

- Staff should check their emails on a regular basis and respond, as appropriate, within a reasonable period if the email is directly addressed to them. Wherever possible, when not in school, staff should set an Automatic Reply (Out of Office) on their email. Where this is not possible, for periods of more than 3 days, the IT Manager may set this for the user.
- Do not enter into any agreement via email unless you are authorised to do so.

## Code of Practice

Steps to consider when sending an email:

- Ask yourself whether you need to send this email. It may be more appropriate to use the telephone or check face to face.
- Limit the number of recipients – only send to those who really need to receive the email.
- Label your email appropriately by changing the sensitivity from Normal to Personal, Private or Confidential within the message options.
- Do not use the Urgent flag unless it really is urgent.
- Use a consistent method of defining a subject line – a clear subject line helps the recipient in filing. Try to keep to one subject for the content of each email – this can make it easier to categorise later if you need to keep it.
- Ensure the email is clearly written – do not use text language or informal language. All content should be professional with suitable language that is not aggressive or inappropriate. Be mindful that others may have different opinions. Ensure you have made it clear how you need the recipient to respond if necessary.
- Never write a whole email in capital letters – this can be interpreted as shouting.
- Spell check before you send
- Sign off with your name and contact details
- Avoid sending attachments. Consider sharing the file location or sending a secure shared link using One Drive.

## Further Guidelines

- Remember – emails remain a written record and can be forwarded to others or printed for formal use. Use the built in protection options of Office 365 to prevent emails being forwarded, modified, printed or copied if required.
- As a rule of thumb, staff are advised to only write what they would say face to face, and should avoid the temptation to respond to an incident or message by email in an uncharacteristic and potentially aggressive fashion. Tone can be misinterpreted on the printed page and once it is sent it could end up in the public domain forever. Email lacks the other cues and clues that convey the sense in which what you say is taken, and you can easily convey the wrong impression.
- Remember that sending email from your school account is similar to sending a letter on Mill Water School letterhead, so don't say anything that might bring discredit or embarrassment to yourself or the school.

## Useful Tip

**New emails:**

1. Create a new email…
2. Fill in the subject line…
3. Compose your message…
4. Avoid sending attachments…
5. Apply message options and protection settings if required…
6. Check everything is correct BEFORE adding any recipients to the email…

*This policy was approved by the Full Governing Body on 25 September 2024*

Mill Water School

Preparation for *their* best future

# Use of Digital Images – Photography and Video Mill Water School Pupils

**To comply with the General Data Protection Regulations 2018, we need your permission before we can photograph or make recordings of your daughter/son.**

We adhere to the following rules for any external use of digital images: If the pupil is named, we avoid using their photograph. If their photograph is used, we avoid naming the pupil.

Where showcasing examples of pupils' work we only use their first names, rather than their full names.

If showcasing digital video work to an external audience, we take care to ensure that the pupils aren't referred to by name on the video and that pupils' full names aren't given in credits at the end of the film.

Only images of pupils in suitable dress are used.

Examples of how digital photography and video may be used include (but are not limited to):

- Your child being photographed (by the classroom teacher, teaching assistant or another child) as part of a learning activity:
    - photographing children at work and then sharing the pictures on the interactive whiteboard in the classroom allowing the children to see their work and make improvements.
    - photographing children at work or engaging in an activity using an iPad or iPod in order to build up evidence for learning for the purposes of formative and summative assessment. These photographs will be shared with parents/carers. Your child's image may also form part of another child's assessment evidence.

- Your child's image being used for presentation purposes around the school:
    - in school wall displays and PowerPoint presentations as part of a project or lesson.

- Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators:
    - within a CDROM/DVD or a document sharing good practice; on our school website.

- Your child's picture appearing in the local media such as newspaper articles about Mill Water, or in very rare cases on television if a film crew attends an event at the school.
- Your child's image being used by local organisations (who have worked with Mill Water) for their marketing purposes, such as the RNLI and the Fire and Rescue Service.
- Your child's image being used by the PTFA on their social media page in order to raise awareness of Mill Water School in the community or to fundraise on behalf of the school.
- Your child's image being used on the Mill Water School social media pages.

In accordance with guidance from the Information Commissioner's Office, parents and carers may take digital images and videos of their children at school events for their own personal use (as such use is not covered by the General Data Protection Regulations). To respect everyone's privacy, and in some cases protection, these images should not be published or made publicly available on social networking sites, nor should parents and carers comment on any activities involving other pupils in the digital images or videos.

**Using Photographs with AAC Devices**

For people with communication difficulties AAC (Alternative & Augmentative Communication) devices can maximise independence, social experiences and reduce frustration from difficulty communicating. Many of these devices use picture symbols and photographs. The devices might be paper forms and laminated in books/folders or they might be on high tech devices like iPads. We would like your permission to put photographs of your child/children into their friends' AAC devices. It would be extremely beneficial to the AAC user to have these photographs so that they can interact with their friends and share news with their family about their day. These AAC devices will be used in and outside of school. The photographs will be used solely for the purpose of supporting communication.

Photographs are stored, shared, used and deleted in accordance with the Mill Water School GDPR Policy.

*This policy was approved by the Full Governing Body on 25 September 2024*

Mill Water School

Preparation for *their* best future

# Use of Digital Images – Photography and Video Consent Form

I have read and understood this document and I agree to the school using photographs of my child, including video material, within the school as part of learning activities and for presentation purposes around the school.

I agree that if I take digital or video images at school events which include images of children other than my own, I will abide by these guidelines in my use of these images.

I also agree for images of my child to be used in the following ways (please tick to indicate your agreement or otherwise):

| | |
|---|---|
| YES ◯ NO ◯ | In presentations about the school and/or Special Partnership Trust and its work in order to share good practice and celebrate its achievements, which may be shown to external audiences such as parents, schools and other educators |
| YES ◯ NO ◯ | On the school and/or Special Partnership Trust's website |
| YES ◯ NO ◯ | On the school and/or Special Partnership Trust's social media page |
| YES ◯ NO ◯ | In local media such as newspaper articles about Mill Water School and/or Special Partnership Trust or, in very rare cases, on television if a film crew attends an event at the school |
| YES ◯ NO ◯ | By local organisations (who have worked with Mill Water School and/or Special Partnership Trust) for their marketing purposes, such as the RNLI and the Fire and Rescue Service |
| YES ◯ NO ◯ | By the Parents, Teachers and Friends Association (PTFA) at fund raising events and on their social media page |
| YES ◯ NO ◯ | Within other pupils' AAC devices |

**Pupil name (s): ……**

**Parents/Carers signature: …….**

**Date: ……**

Mill Water School
Preparation for *their* best future

# Use of Digital Images – Photography and Video
# Mill Water School Staff

**To comply with the General Data Protection Regulations 2018, we need your permission before we can take, store and use your photograph**

Examples of how digital photography and video may be used include:

- Your photograph being taken specifically to be used on your ID badge and the same image being stored on SIMS, our School Information Management System. This image will be linked with your name. It will be updated every two to three years and deleted 7 years after you leave employment at the school, along with your online personnel record. You can ask for it to be deleted before this date. This photograph may be shared with LEA representatives but will not be shared with any other third party.
- Your photograph/video being taken alongside that of a pupil, as evidence of their learning or participation in an activity. This image will be taken using a school camera, iPad or iPod and will be stored securely on the school system. Photographs of children and associated adults will normally be deleted after two years. Your first name may be linked to the photograph. The photograph may be shared with parents/carers as part of our electronic home school communication, via Class Dojo, Evidence for Learning or Tapestry. It could also be posted on our school website or school Facebook page.
- You may be photographed or videoed if you support pupils in any school or class production.
- Your image may appear alongside that of a pupil in a presentation/newsletter about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators: within a CDROM/DVD or a document sharing good practice; on our school website; on the school Facebook page; in the local media or, in very rare cases, on television if a film crew attends an event at the school
- Your image, alongside that of a child's, being used by local organisations (who have worked with Mill Water) for their marketing purposes, such as the RNLI and the Fire and Rescue Service
- Your image, alongside that of a child's, being used by the PTFA on their social media page in order to raise awareness of Mill Water School in the community or to fundraise on behalf of the school
- Your image may be included on a child's AAC device.

*This policy was approved by the Full Governing Body on 25 September 2024*

Mill Water School
Preparation for *their* best future

# Use of Digital Images – Photography and Video Staff Consent Form

I have read and understood this document and I agree to the school using my image in the following ways:

| | |
|---|---|
| YES ◯ NO ◯ | As part of the school's evidence for learning process and home school communication |
| YES ◯ NO ◯ | In an around the school, including the display board in front reception area |
| YES ◯ NO ◯ | In presentations about the school and/or Special Partnership Trust and its work in order to share good practice and celebrate its achievements, which may be shown to external audiences such as parents, schools and other educators |
| YES ◯ NO ◯ | On the school and/or Special Partnership Trust's website |
| YES ◯ NO ◯ | On the school and/or Special Partnership Trust's social media page |
| YES ◯ NO ◯ | As part of a school production |
| YES ◯ NO ◯ | In local media such as newspaper articles about Mill Water School and/or Special Partnership Trust or, in very rare cases, on television if a film crew attends an event at the school |
| YES ◯ NO ◯ | By local organisations (who have worked with Mill Water School and/or Special Partnership Trust) for their marketing purposes, such as the RNLI and the Fire and Rescue Service |
| YES ◯ NO ◯ | By the Parents, Teachers and Friends Association (PTFA) at fund raising events and on their social media page |
| YES ◯ NO ◯ | Within other pupils' AAC devices |

**Name: ……**

**Signature: ……..**

**Date: ……..**

# Legislation

## Computer Misuse Act 1990

This Act makes it an offence to:

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

## Data Protection Act 1998

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

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

## The Data Protection Act 2018

Updates the 1998 Act, incorporates the General Data Protection Regulations (GDPR) and aims to:

- Facilitate the secure transfer of information within the European Union.
- Prevent people or organisations from holding and using inaccurate information on individuals. This applies to information regarding both private lives or business.
- Give the public confidence about how businesses can use their personal information.
- Provide data subjects with the legal right to check the information businesses hold about them. They can also request for the data controller to destroy it.
- Give data subjects greater control over how data controllers handle their data.
- Place emphasis on accountability. This requires businesses to have processes in place that demonstrate how they're securely handling data.
- Require firms to keep people's personal data safe and secure. Data controllers must ensure that it is not misused.
- Require the data user or holder to register with the Information Commissioner.

All data subjects have the right to:

- Receive clear information about what you will use their data for.
- Access their own personal information.
- Request for their data to be revised if out of date or erased. These are known as the right to rectification and the right to erasure
- Request information about the reasoning behind any automated decisions, such as if computer software denies them access to a loan.
- Prevent or query about the automated processing of their personal data.

## Freedom of Information Act 2000

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

## Communications Act 2003

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

## Malicious Communications Act 1988

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

## Regulation of Investigatory Powers Act 2000

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

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

## Trade Marks Act 1994

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

## Copyright, Designs and Patents Act 1988

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

## Telecommunications Act 1984

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

## Criminal Justice & Public Order Act 1994

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

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

## Racial and Religious Hatred Act 2006

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

## Protection from Harassment Act 1997

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

## Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

## Sexual Offences Act 2003

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

## Public Order Act 1986

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

## Obscene Publications Act 1959 and 1964

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

## Human Rights Act 1998

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

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

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

## The Education and Inspections Act 2006

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

## The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

## The Protection of Freedoms Act 2012

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

## The School Information Regulations 2012

Requires schools to publish certain information on its website:

https://www.gov.uk/guidance/what-maintained-schools-must-publish-online

## Serious Crime Act 2015

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

## Criminal Justice and Courts Act 2015

Revenge porn – as it is now commonly known – involves the distribution of private and personal explicit images or video footage of an individual without their consent, with the intention of causing them embarrassment and distress. Often revenge porn is used maliciously to shame ex-partners. Revenge porn was made a specific offence in the Criminal Justice and Courts Act 2015. The Act specifies that if you are accused of revenge porn and found guilty of the criminal offence, you could be prosecuted and face a sentence of up to two years in prison.

For further guidance or support please contact the Revenge Porn Helpline