# Turnfurlong Infant School

# E-Safety Policy – 2023-2024

At Turnfurlong Infant School, we see E-safety (electronic safety) as a fundamental part of children's education. E-safety is not just concerned with the internet, it's also about mobile devices and game consoles. We believe that these procedures set out to make our pupils effective Digital Citizens who understand the dangers around them and can make effective reasoned choices in order to keep themselves safe.

In a rapidly changing digital world we believe that this policy should be developed and reviewed annually.

## 1. Scope of the Procedures:

These procedures apply to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school IT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, peer on peer abuse or other e-safety incidents covered by these procedures, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data.

The school will deal with such incidents within these procedures and associated behaviour and anti-bullying (including cyber bulling) policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

## 2. Education and Training

### 2.1 Pupils

Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience. E-safety is a focus in all areas of the curriculum and staff reinforce e-safety messages across the curriculum. The e-safety curriculum ensures that:

- E-safety is part of a planned curriculum which provides progression
- Key e-safety messages are reinforced as part of assemblies
- Pupils are taught in all lessons to be critically aware of the materials / content they access on-line. 'Zip it, Block it, Flag it'.
- Pupils are encouraged to adopt safe and responsible practices both within and outside school
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit. Many sites are blocked however teachers must remain vigilant about the content enabled.

### 2.2 Parents / Carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- Letters, newsletters, web site
- Parents / Carers workshop
- High profile events / campaigns e.g. Safer Internet Day, Online Safety week
- Reference to relevant web sites / publications

### 2.3 Staff / Volunteers

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in these procedures. Training will be offered as follows:

- A planned programme of e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety procedures and Acceptable Use Agreements.
- These E-Safety procedures and their updates will be presented to and discussed by staff in staff / year group meetings, and/ or INSET days.
- The Computing Co-ordinator will provide advice / guidance / training to individuals as required.

### 2.4 Governors

Governors should have an awareness of e-safety as part of their safeguarding training and monitor the implementation of this policy. This may take place in a number of ways:

- Attendance at a training event
- Attendance of a lesson
- Attendance of a school e-safety assembly

## 3 Roles and Responsibilities:

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

### 3.1 Governors:

Governors are responsible for the approval of the E-Safety Procedures and for reviewing the effectiveness of the procedures. This will be carried out by the Governors and P&C Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Safeguarding Governor. The role of the Safeguarding Governor will include:

- Regular meetings with the Computing Co-ordinator
- Regular monitoring of e-safety incident logs
- Reporting to relevant Governors

### 3.2 Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the Computing Co-ordinator.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff
- The Headteacher is responsible for ensuring that the Computing Co-ordinator and other relevant staff receive suitable training to enable them to carry out their PREVENT and e-safety roles and to train other colleagues, as relevant.
- The Senior Leadership Team will receive regular updates from the Computing Co-ordinator.

### 3.3 Computing Co-ordinator:

- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety procedures / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff
- Liaises with the Local Authority / relevant body
- Liaises with school technicians
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- Meets regularly with Safeguarding Governor to discuss current issues, review incident logs and filtering / change control logs
- Attends relevant meetings
- Reports regularly to Senior Leadership Team

### 3.4 Technical staff:

Technicians will ensure that:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack
- That the school meets required e-safety technical requirements
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- That they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant

- that the use of the network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher and/or Computing Co-ordinator for investigation

### 3.5 Teaching and Support Staff:

Are responsible for ensuring that:

- They have an up to date awareness of PREVENT, e-safety matters, and of the current e-safety procedures and practices
- They have read, understood and signed the Computing Security agreement
- They report any suspected misuse or problem to the Headteacher / Computing Co-ordinator for investigation
- All digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
- E-safety issues are embedded in all aspects of the curriculum and other activities
- Pupils understand and follow the e-safety and acceptable use procedures
- Pupils have a good understanding of research skills
- Pupils understand that information on the internet is not always reliable
- They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current procedures with regard to these devices
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

### 3.6 Designated Safeguarding Lead (DSL):

Technology provides additional means for child protection issues to arise therefore, we believe that the DSL should be trained in e-safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- Access to illegal / inappropriate materials
- Sharing of personal data and GDPR
- Cyber-bullying
- Peer on peer abuse
- Child Sexual Exploitation
- Female Genital Mutilation
- Extremism, terrorism and Radicalisation
- Inappropriate on-line contact with adults / strangers
- Upskirting (cameras and mobile phones)
- Potential or actual incidents of grooming

### 3.7 Pupils:

- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so. ‘Zip it, Block it, Flag it!’

- Will be expected to know and understand procedures on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images, peer on peer abuse and on cyber-bullying.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Procedures covers their actions out of school.

### 3.8 Parents/Carers:

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of digital and video images taken at school events.

## 4 Technical – infrastructure / equipment, filtering and monitoring

The school uses JSL Services group Ltd for its computing requirements. Whilst the computing Co-ordinator has overall responsibility, together, the school and JSL ensure that the school's infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within these procedures are implemented.

- School/technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school / technical systems and devices
- The technicians and the Computing Co-ordinator are responsible for ensuring that software licence logs are accurate and up to date.
- Content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.
- School/technical staff regularly monitor and record the activity of users on the school systems and users are made aware of this in the staff code of conduct.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software (Sophos).
- Staff are not permitted to download executable files and install programmes on school devices. Should this be necessary, staff members should consult either the computing co-ordinator or the school's technician.
- The use of removable media (e.g. memory sticks) is not permitted by users on school devices (awaiting a suitable solution for file sharing).
- Bring Your Own Device (BYOD) are not permitted within school.

## 5 Use of digital and video images

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

- **When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.**
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance and consent on the use of such images.
- 'Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Consent from parents or carers will be obtained before photographs of pupils are published on any media forum.

## 6 Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 which states that personal data must be:

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

The school ensures that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the “Privacy Notice” and lawfully processed in accordance with the “Conditions for Processing”.
- It has a Data Protection Policy
- Jai Lablans, of JSL is named as its Data Protection Officer (DPO).
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- It has clear and understood arrangements for the security, storage and transfer of personal data
- There are clear and understood procedures and routines for the deletion and disposal of data
- There are procedures for reporting, logging, managing and recovering from information risk incidents
- There are clear procedures about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner’s Office (ICO).

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.

## 7 Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems.
- Users must immediately report, to the e-safety Co-ordinator the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and parents / carers (email, parent mail etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems.
- Pupils should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies. ‘Zip it, block it, Flag it’ is used as the pupils primary e-safety message.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

## 8 Social Media - Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes procedures that set out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of pupils, the school and the individual when publishing any material online. Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012' and all staff are expected to adhere to the school's code of conduct.

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school / or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place. The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

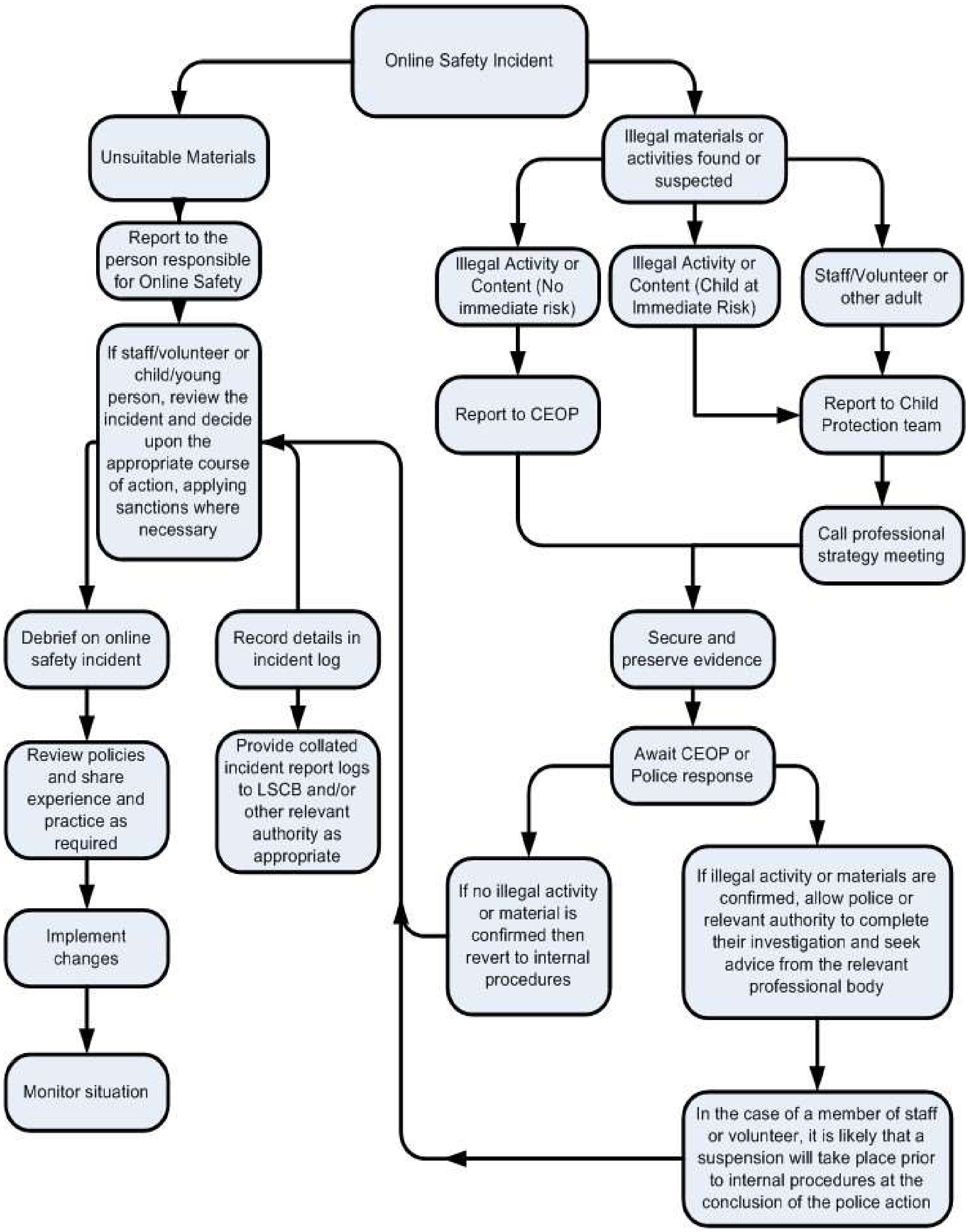
- Training to include: acceptable use; social media risks; checking of settings
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk. School staff should ensure that:
  - ❖ No reference should be made in social media to pupils or parents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

## 9 Responding to incidents of misuse

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

### Illegal Incidents

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


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

## Other Incidents

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

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

- Has more than one member of staff / volunteer been involved in this process? This is vital to protect individuals if accusations are subsequently reported.

- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse)
- 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 Designated Officer for Safeguarding (LADO) or national / local organisation (as relevant).
- Police involvement and/or action
- If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
- incidents of ‘grooming’ behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

## School / Actions & Sanctions

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

Pupils Actions / Sanctions

| Incidents: | Refer to class teacher | Refer to Year Leader | Refer to Headteacher | Refer to Police | Refer to technician re filtering / security etc. | Inform parents / carers | f network / internet access | Warning | Further sanction e.g. exclusion |
|---|---|---|---|---|---|---|---|---|---|
| **Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).** | | ⍰ | ⍰ | ⍰ | | | | | |
| Unauthorised use of non-educational sites during lessons | | ⍰ | | | | | | | |
| Unauthorised use of digital camera / other mobile device | | | ⍰ | | | | | | |
| Unauthorised downloading or uploading of files | | ⍰ | | | | | | | |
| 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 | | ⍰ | ⍰ | ⍰ | | | | | |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school | | | ⍰ | | | | | | |
| Using proxy sites or other means to subvert the school's filtering system | | | ⍰ | ⍰ | ⍰ | | | | |
| Accidentally accessing offensive or pornographic material and failing to report the incident | | | ⍰ | | | | | | |
| Deliberately accessing or trying to access offensive or pornographic material | | | ⍰ | ⍰ | | | | | |

## Staff Actions / Sanctions

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

### Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media,

The school will comply with the Data Protection Act and request parents / carers permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

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

This policy was reviewed by the Governors – 14th September 2023

Review Date – Autumn Term 202