# Orton Wistow Primary School
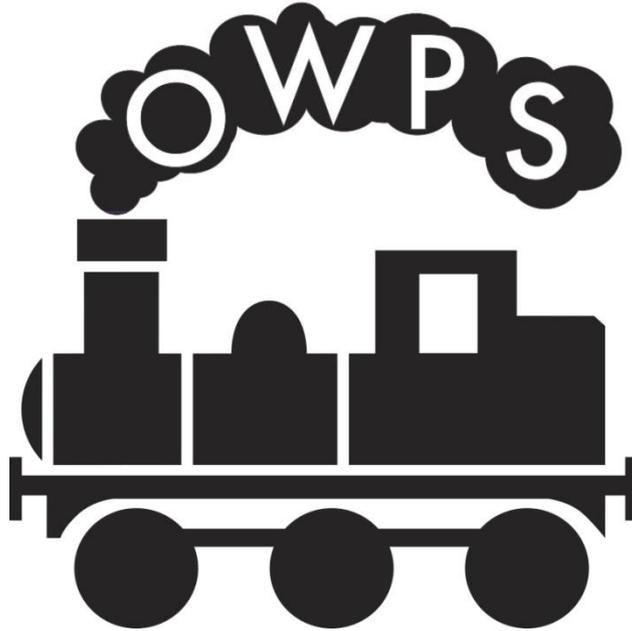


## Online Safety Policy

| Status | Recommended |
|---|---|
| GB Monitor | FGB |
| Staff Lead | Working group |
| Senior Lead | Online Safety Lead |
| Version | EPM Model |
| Publication Date | Sum 19 |
| Next Review | Sum 20 |

| | |
|---|---|
| Date Agreed: | |
| Headteacher: | |
| Chair of Governors: | |

## Development / Monitoring / Review of this Policy

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

- Deputy Headteacher / Online Safety Lead
- Staff – including Teachers, Support Staff, Technical staff
- Governor
- Parents and Carers

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

## Schedule for Development / Monitoring / Review

| | |
|---|---|
| This Online Safety policy was approved by the Board of Directors / Governing Body / Governors Sub Committee on: | 29th April 2019 |
| The implementation of this Online Safety policy will be monitored by: | **Colin Marks** ( Online Safety Lead) |
| Monitoring will take place at regular intervals: | **Spring term – Annually** |
| The Governing Body will receive a report on the implementation of the Online Safety Policy (which will include anonymous details of online safety incidents) at regular intervals: | **Summer Term – Annually** |
| 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: | **Spring 2020** |
| Should serious online safety incidents take place, the following external persons / agencies should be informed: | LA Safeguarding Officer **Stuart Mansell** Academy CEO **PCSO Jan UPEX** Police |

The school will monitor the impact of the policy using:

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

## Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students / 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 online-bullying or other Online Safety incidents covered by this policy, which may take place outside of the *school* , but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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

## Roles and Responsibilities

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

## Governors

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

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

## Headteacher and Senior Leaders

- The *Headteacher* has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the *Online Safety Lead*.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant *Local Authority / MAT / other relevant body* disciplinary procedures).
- *The Headteacher / Senior Leaders are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.*

- *The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.*
- *The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead.*

## Online Safety Lead

- leads the Online Safety Group
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority / MAT / relevant body
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meets regularly with Online Safety *Governor* to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting of *Governors*
- reports regularly to Senior Leadership Team

## Network Manager / Technical staff

The Network Manager / Technical Staff is responsible for ensuring:

- **that the *school's* technical infrastructure is secure and is not open to misuse or malicious attack**
- **that the *school* meets required online safety technical requirements and any *Local Authority / MAT / other relevant body* Online Safety Policy / Guidance that may apply.**
- **that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed**
- *the filtering policy (if it has one), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person*
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- *that monitoring software / systems are implemented and updated as agreed in school policies*

## Teaching and Support Staff

Are responsible for ensuring that:

- **they have an up to date awareness of online safety matters and of the current** *school* **Online Safety Policy and practices**
- **they have read, understood and signed the Staff Acceptable Use Policy (AUP)**
- **they report any suspected misuse or problem to the** *Online Safety Lead* **for investigation**
- **all digital communications with pupils / parents / carers should be on a professional level** *and only carried out using official school systems*
- online safety issues are embedded in all aspects of the curriculum and other activities
- students understand and follow the Online Safety Policy and acceptable use policies
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- *in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches*

## Designated Safeguarding Lead

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

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

## Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the *school* community, with responsibility for issues regarding online safety and monitoring the Online Safety Policy including the impact of initiatives. Depending on the size or structure of the *school* this group may be part of the safeguarding group. The group will also be responsible for regular reporting to the *Governing Body*.

Members of the Online Safety Group will assist the Online Safety Lead with:

- the production / review / monitoring of the school Online Safety Policy.

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

### Pupils:

- **are responsible for using the *school* digital technology systems in accordance with the Pupil Acceptable Use Agreement**
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the *school's* Online Safety Policy covers their actions out of school, if related to their membership of the school

### Parents / Carers

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

- digital and video images taken at school events
- access to parents' sections of the website and on-line pupil records

## Policy Statements

### Education – Students / Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating *pupils* to take a responsible approach. The education of *pupils* in online safety / digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- **A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited**
- **Key online safety messages should be reinforced as part of a planned programme of assemblies**
- **Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.**
- **pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet**
- **pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.**
- *pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.*
- *Staff should act as good role models in their use of digital technologies, the internet and mobile devices*
- *in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.*
- *Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.*
- *It is accepted that from time to time, for good educational reasons, pupils may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.*

## Education – Parents / Carers

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

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

- *Curriculum activities*
- *Letters, newsletters, web site*
- *Parents / Carers evenings / sessions*
- *High profile events / campaigns e.g. Safer Internet Day*
- *Reference to the relevant web sites / publications e.g. [swgfl.org.uk](swgfl.org.uk) [www.saferinternet.org.uk/](www.saferinternet.org.uk/)  [http://www.childnet.com/parents-and-carers](http://www.childnet.com/parents-and-carers)*

### Education & Training – Staff / Volunteers

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

- **A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.**
- **All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.**
- *The Online Safety Lead (or other nominated person) will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.*
- *This Online Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.*
- *The Online Safety Lead will provide advice / guidance / training to individuals as required.*

## Training – Governors

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

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

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

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

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

- **School technical systems will be managed in ways that ensure that the school meets recommended technical requirements**
- **There will be regular reviews and audits of the safety and security of school technical systems**
- **Servers, wireless systems and cabling must be securely located and physical access restricted**
- **All users will have clearly defined access rights to school technical systems and devices.**
- **All users** *(at KS2 and above)* **will be provided with a username and secure password by** Simon Hollingsworth *who will keep an up to date record of users and their usernames.* **Users are responsible for the security of their username and password**
- The "administrator" passwords for the school ICT systems, used by the Network Manager (or other person) must also be available to the *Headteacher* or other nominated senior leader and kept in a secure place (eg school safe)
- Simon Hollingsworth (ICT Support technician) is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- **Internet access is filtered for all users.**
- **Internet filtering / monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.**
- *The school has provided enhanced / differentiated user-level filtering*
- 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.

## Mobile Technologies (including BYOD/BYOT)

Mobile technology devices may be school owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include cloud based services such as email and data storage.

All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe

and appropriate use of mobile technologies should be an integral part of the school's Online Safety education programme.

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

| | School Devices | | | Personal Devices | | |
|---|---|---|---|---|---|---|
| | School owned for single user | School owned for multiple users | Authorised device[1] | Student owned | Staff owned | Visitor owned |
| Allowed in school | Yes | Yes | Yes | No | Yes | Yes |
| Full network access | Yes | Yes | No | No | Yes | No |
| Internet only | No | No | Yes | No | No | Yes |
| No network access | Yes | Yes | Yes | Yes | No | Yes |

## Use of digital and video images

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

- **When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.**
- **Written permission from parents or carers will be obtained before photographs of pupils are published on the school website / social media / local press**
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school / academy events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in

some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other *students* / *pupils* in the digital / video images.

- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

## Data Protection

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

**The school must ensure that:**

- **It has a Data Protection Policy.**
- **It has paid the appropriate fee to the Information Commissioner's Office (ICO).**
- **It has appointed a Data Protection Officer (DPO).**
- **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.**
- **Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.**
- **The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice.**
- **Where special category data is processed, a lawful basis and a separate condition for processing have been identified.**
- **Data Protection Impact Assessments (DPIA) are carried out.**
- **It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.**

- **Procedures must be in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller.**
- **There are clear and understood data retention policies and routines for the deletion and disposal of data.**
- **There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.**
- **Consideration has been given to the protection of personal data when accessed using any remote access solutions.**
- **All schools must have a Freedom of Information Policy which sets out how it will deal with FOI requests.**
- **All staff receive data handling awareness / data protection training and are made aware of their responsibilities.**

Staff must ensure that they:

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

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

- **The data must be encrypted and password protected.**
- The device must be password protected.
- **The device must offer approved virus and malware checking software.**
- **The data must be securely deleted from the device, in line with school / academy policy (below) once it has been transferred or its use is complete.**

## Communications

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

| Communication Technologies | 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 |
| Mobile phones may be brought to the school | x | | | | | | | x |
| Use of mobile phones in lessons | | | | x | | | | x |
| Use of mobile phones in social time | | x | | | | | | x |
| Taking photos on mobile phones / cameras | | | | x | | | | x |
| Use of other mobile devices e.g. tablets, gaming devices | | | | x | | | | x |
| Use of personal email addresses in school , or on school network | | | | x | | | | x |
| Use of school email for personal emails | | x | | | | | | x |
| Use of messaging apps | | | | x | | | | x |
| Use of social media | | x | | | | | | x |
| Use of blogs | | x | | | | x | | |

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

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

- *Personal information should not be posted on the school / academy website and only official email addresses should be used to identify members of staff.*

## Social Media - Protecting Professional Identity

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

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

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

School staff should ensure that:

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

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

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

Monitoring of Public Social Media

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school

- The school should effectively respond to social media comments made by others according to a defined policy or process

## Dealing with unsuitable / inappropriate activities

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

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

| User Actions | | Acceptable | Acceptable at certain times | Acceptable for nominated | Unacceptable | Unacceptable and illegal |
|---|---|:---:|:---:|:---:|:---:|:---:|
| Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to: | Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978 | | | | | X |
| | Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003. | | | | | X |
| | Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008 | | | | | X |
| | Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986 | | | | | X |
| | Pornography | | | | X | |
| | Promotion of any kind of discrimination | | | | X | |
| | threatening behaviour, including promotion of physical violence or mental harm | | | | X | |
| | Promotion of extremism or terrorism | | | | X | |

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

## Responding to incidents of misuse

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

## Illegal Incidents

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

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

## Other Incidents

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

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

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority / Academy Group or national / local organisation (as relevant).
    - Police involvement and/or action
- **If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the *school / academy* and possibly the police and demonstrate that visits to

these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

## School / Academy Actions & Sanctions

It is more likely that the school / academy 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:

**Actions / Sanctions**

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

| Staff Incidents | Refer to line manager | Refer to Headteacher | Refer to Local Authority / HR | Refer to Police | Refer to Technical Support Staff for action re filtering | Warning | Suspension | Disciplinary action |
|---|:---:|:---:|:---:|:---:|:---:|:---:|:---:|:---:|
| Attempting to access or accessing the school network, using another pupil's account | X | X | | | | | X | |
| Attempting to access or accessing the school network, using the account of a member of staff | X | X | | | X | | X | |
| Corrupting or destroying the data of other users | X | X | | | X | | X | |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | X | X | X | | X | | | X |
| Continued infringements of the above, following previous warnings or sanctions | X | X | X | | X | | | X |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school | X | X | X | | X | | X | |
| Using proxy sites or other means to subvert the school's filtering system | X | X | X | X | X | | X | |
| Accidentally accessing offensive or pornographic material and failing to report the incident | X | X | X | X | X | | X | |
| Deliberately accessing or trying to access offensive or pornographic material | X | X | X | X | X | | X | X |
| Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act | X | X | | X | X | | X | |

**Actions / Sanctions**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).** | | X | X | X | X | | | X |
| Inappropriate personal use of the internet / social media / personal email | X | X | | | | X | | |
| Unauthorised downloading or uploading of files | X | X | | | | X | | |
| Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account | X | X | | | X | X | | |
| Careless use of personal data e.g. holding or transferring data in an insecure manner | X | X | | | | X | | |
| Deliberate actions to breach data protection or network security rules | X | X | | | X | | | X |
| Corrupting or destroying the data of other users or causing deliberate damage to hardware or software | X | X | | | X | | | X |
| Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature | X | X | | | X | | | X |
| Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils | X | X | | | X | | | X |
| Actions which could compromise the staff member's professional standing | X | X | | | | X | | |
| Actions which could bring the school into disrepute or breach the integrity of the ethos of the school | X | X | | | | X | | |
| Using proxy sites or other means to subvert the school's filtering system | X | X | | | X | X | | |
| Accidentally accessing offensive or pornographic material and failing to report the incident | X | X | | | X | | | X |
| Deliberately accessing or trying to access offensive or pornographic material | X | X | | | X | | | X |
| Breaching copyright or licensing regulations | X | X | | | X | | | X |
| Continued infringements of the above, following previous warnings or sanctions (*) | X | X | | | | | | X |

\* This could result in suspension

## 1. Terms of Reference

1.1. This procedure applies to all employees regardless of their permanent, fixed-term, full or part-time status.

1.2. Definitions:

"Headteacher" also refers to any other title used to identify the Headteacher, where appropriate, or other Senior Manager delegated to deal with the matter by the Headteacher.

"Companion" refers to a person chosen by the employee to accompany them at a Formal Hearing, who shall be a trade union representative or a workplace colleague.

"Probationer" refers to the employee who is serving the probation period.

"Line Manager" refers to the person delegated to manage the probation period. This may be a Senior Manager other than the direct Line Manager.

"Governors Disciplinary Committee" may be convened for a Formal Hearing where the Headteacher considers that they must act in the role of Line Manager. In this event substitute 'Headteacher' with 'Governors Disciplinary Committee' throughout the procedure.

"Governors Appeal Committee" may be convened to hear an appeal against a decision to dismiss. Where possible the number of governors on the committee will be equal to, or greater than, the decision maker(s) of the case being appealed.

"Formal Hearing" a meeting at which a recommendation to dismiss the Probationer is considered.

## 2. Introduction

2.1. This procedure is non contractual and for guidance only, although reduced notice of termination provisions by the employer are covered in the contract of employment. The exception to this is substantiated allegations of gross misconduct, as outlined in paragraph 4.3 below, which normally warrants summary dismissal without notice.

2.2. It is the responsibility of the Line Manager to implement the procedure and to ensure that the procedure is communicated to Probationers and that it is applied consistently.

2.3. The probation period is for six months from the start date of employment and may be extended by an additional three months, or longer if the extension period includes school holidays (see section 4.8).

2.4. It may also be agreed at the outset of the employment that the probation period will be longer than six months where the Probationer is employed on a term time only contract and the probation period spans the school summer holidays.

2.5. The purpose of the probation period is to enable an assessment to be made regarding a Probationer's suitability for the job for which they have been employed.

2.6. The probation procedure provides a consistent and fair framework for:

2.6.1. Monitoring and reviewing the performance of new employees in relation to:

- Quality of work and understanding of role
- Attitudes and motivation
- Conduct and attendance
- Compliance with all policies and procedures particularly those relating to safeguarding and promoting the welfare of children and young people

- Health and safety

2.6.2. Providing feedback and opportunity for discussion.

2.6.3. A structured approach to address any concerns linked to 2.6.1.

2.7. The capability, disciplinary and sickness absence policies and/or procedures do not apply during the probation period. If issues of conduct, poor performance or sickness arise during the probation period, the probation procedure will normally be used to address such matters. Where allegations have been made against a Probationer, a management investigation will be conducted into the matter. In cases of alleged serious misconduct the Headteacher (or person with delegated responsibility for suspension) will normally suspend the Probationer pending an investigation.

2.8. The following employees are excluded from a probationary period:

- When transferring between the Trust's Academies
- Following an internal promotion
- Following any variations to the terms and conditions of employment
- Newly Qualified Teachers where separate arrangements exist.

[The NQT induction arrangements and the appraisal policy for teachers will run concurrently with the probation period. The Line Manager will normally be the induction tutor/appraiser. Where deemed necessary the probation procedure will take precedence over the appraisal policy.]

## 3. Equality and Diversity

3.1. The procedure will be operated in accordance with our Equality and Diversity Policy. We are committed to developing, maintaining and supporting a culture of equality and diversity in employment. The impact of the procedure will be monitored in accordance with the Equality Act 2010.

## 4. The Procedure

4.1. The Line Manager is responsible for ensuring that the Probationer is properly monitored during the probation period and meetings and paperwork are completed in a timely manner. The Probationer will be provided with a copy of the procedure and indicative dates for the probation meetings. In the event that the Probationer's standards fall below expectations, the Line Manager is responsible for initiating and taking action in accordance with this procedure.

4.2. The Line Manager should, in normal circumstances, conduct three reviews with the Probationer. Reviews should take the form of a confidential meeting between the Line Manager and the Probationer, in which there is opportunity for two-way discussion.

4.3. In exceptional circumstances, where there are serious concerns over the suitability of a Probationer, the Line Manager may decide to progress straight to the Final Review and omit the Second Review, or to reduce the time between the review meetings. Such concerns may include substantiated safeguarding or health and safety concerns or substantiated allegations that may constitute gross misconduct or during an extended probation period.

4.4. **The First Review:** To be completed within weeks four to six of the Probationer's start date.

The purpose of this meeting is for the Line Manager to evaluate the Probationer's performance and discuss any key issues. If improvements in performance are required, full details should be given, including appropriate management support/training.

Upon completion of this review meeting, the Line Manager should complete the Probation Period Review Form (Appendix 1). This should be signed by the Line Manager and the Probationer. A copy should be given to the Probationer and a copy saved on the personnel file.

4.5. **The Second Review:** On completion of three months service.

The purpose of this meeting is to review the Probationer's performance over the first three months. Where the First Review indicated that improvements in performance were required, the Second Review meeting should be used to consider the extent of any improvement that may or may not have taken place.

Where the Probationer has not met the required standards, they will be informed that continued failure to meet those standards could result in dismissal.

Upon completion of this meeting, the Line Manager should complete the Probation Period Review Form (Appendix 1). This should be signed by the Line Manager and the Probationer, and a copy should be given to the Probationer and a copy saved on the personnel file.

4.6. **The Final Review:** On completion of five months service.

Prior to the Final Review meeting, which normally takes place after the Probationer has completed five months service, the Line Manager should decide whether:

4.6.1. The Probationer has passed probation or;

4.6.2. The probation period is extended due to exceptional circumstances. Consideration to extend may include the following, but this is not an exhaustive list:

- Performance concerns have not been fully addressed but there is a reasonable expectation that satisfactory performance standards may be met by the end of an extension of the probation period.
- The Probationer has had an extended period of permitted absence and it has not been possible to assess performance.
- Other exceptional circumstances.

4.6.3. Recommendation to the Headteacher at a Formal Hearing that the Probationer is dismissed.

4.7. **The Probationer has passed probation**

Upon completion of the final review meeting, if the Probationer has passed probation the Line Manager will complete the Probation Period Review Form (Appendix 2). This will be signed by the Line Manager and the Probationer. The form should be placed on the Probationer's personnel file with a copy provided to the employee.

4.8. **The Probation period is extended**

Where the decision is to extend the probation period, this will normally be limited to one extension and the extension will be no longer than three months unless the extension period includes school holidays, in which case it may be longer.

Before extending the probation period, the Line Manager will normally seek HR advice. The Line Manager will confirm the terms of the extension in writing to the Probationer, including:

- The length of the extension, the date on which the extension will end and dates of review meetings, adjusted according to the extension.
- The reason for the extension and, if the reason is unsatisfactory performance, details of how and why performance has fallen short of the required standards.

- The performance standards or objectives that the employee is required to achieve by the end of the extended period of probation.
- Any support, for example further training, that will be provided during the extended period of probation and a statement that, if the employee does not fully meet the required standards by the end of the extended period of probation, the employment will be terminated.

There is no right of appeal to the extension of a probation period.

4.9. **Headteacher's Formal Hearing**

If the Line Manager decides to recommend to the Headteacher at a Formal Hearing that the Probationer is dismissed then they will write to the Probationer to inform them as soon as practicably possible, at least 5 working days in advance, setting out:

a) The date, time and place of the Formal Hearing.

b) That the purpose of the Formal Hearing is to recommend dismissal and the reasons why.

c) The Probationer's right to be accompanied by a Companion.

d) The titles of enclosed copies of any documents which may be considered.

e) The name and position of any other person present at the meeting e.g. note taker or HR Adviser.

The Probationer must advise the Line Manager of the following at least 3 working days in advance of the Formal Hearing:

a) The name and designation of any Companion.

b) Any written documentation to be considered.

The Probationer, who may be accompanied by a Companion, will have the opportunity to state their case, before a decision is made.

The Headteacher may decide:

a) To terminate employment from the date of the Formal Meeting with probation period notice.
b) Extend the probation period. This will revert the process back to the Line Manager.
c) Consider deployment to a suitable available alternative post (in which case a new shortened probation period will be put in place and the schedule and number of review meetings adjusted accordingly).

The Headteacher will write to the Probationer confirming the decision within 5 working days of the hearing.

## 5. Right of Appeal

5.1. The Probationer has a right of appeal against a decision to dismiss.

5.2. An appeal should be made in writing to the Clerk to the Governors, stating the grounds for appeal in full, within 5 working days of the date of the written decision.

5.3. An appeal will be heard by the Governors Appeal Committee, none of whom shall have any previous involvement in the case. The Governors Appeal Committee may have an HR Adviser present.

5.4. An appeal hearing will, in normal circumstances, be heard within 10 working days after receipt of the appeal. The Clerk to Governors will usually undertake administrative arrangements for any appeal

hearing. The outcome will be confirmed in writing as soon as possible and usually within 5 working days of the appeal hearing. There will be no further right of appeal.

Appendix 1

## Probation Period Review

| Review Meeting: | First | Second | Final | Extension |
|---|---|---|---|---|
| **Date:** | | | | |

This form should be completed by the Probationer's Line Manager after each Review Meeting. This should be signed by the Line Manager and the Probationer, and the original placed on the personnel file with a copy to the Probationer.

Probationer's Name: _____

Start Date: _____

Job Title:_____

Line Manager's Name:_____

Line Manager's Job Title: _____

Review of:

| | Exceeds expectations | As expected | Below expectation |
|---|---|---|---|
| **Quality and accuracy of work** | | | |
| **Efficiency/work rate** | | | |
| **Attendance** | | | |
| **Time Keeping** | | | |
| **Work relationships (team work and interpersonal communication skills)** | | | |
| **Competency in the job** | | | |
| **Understanding of the job** | | | |
| | | | |
| | | | |

Line Manager's Comments:_____

_____

_____

_____

_____

_____

_____

_____


Probationer's Comments: _____

_____

_____

_____

_____

_____

_____

_____


Objectives for Next Review: _____

_____

_____

_____

_____

_____

_____

_____


Line Manager's Signature:_____

Date: _____

Probationer's Signature: _____

Date: _____

## Probation Period Review: For Completion following Final Review

**Probation Passed** ☐

Line Manager's Comments:_____

_____

_____

_____

_____

_____

_____

_____

**Probation Extended** ☐

*If the probation is extended then an account of the concerns and a support plan for the extension period will be attached to this form.*

Line Manager's Reasons: _____

_____

_____

_____

_____

_____

_____

_____

**Formal Hearing:** Recommendation to the Headteacher that the Probationer is dismissed ☐

*A statement of reasons will be attached to this form.*

Line Manager's Signature:_____

Date: _____

Probationer's Signature: _____

Date: _____