

# Penketh Primary School

## Online Safety Policy



# Contents

Penketh Primary School .....	0
Online Safety Policy .....	0
Contents.....	1
<b>Introduction</b> .....	2
<b>Development/Monitoring/Review of this Policy</b> .....	4
Roles and Responsibilities .....	5
<b>Policy Statements</b> .....	8
<b>Communications</b> .....	14
<b>Dealing with unsuitable/inappropriate activities</b> .....	16
Responding to incidents of misuse .....	18
<b>Illegal Incidents</b> .....	18
Other Incidents.....	20
School actions & sanctions.....	<b>Error! Bookmark not defined.</b>
Appendix.....	21
Pupil Acceptable Use Agreement – for older students/pupils .....	22
Pupil Acceptable Use Policy Agreement – for younger pupils (Foundation/KS1) .....	25
Parent/Carer Acceptable Use Agreement.....	26
Staff (and Volunteer) Acceptable Use Policy Agreement Template .....	29
Responding to incidents of misuse – flow chart.....	32
Record of reviewing devices/internet sites (responding to incidents of misuse) .....	33
Reporting Log.....	34
Training Needs Audit Log.....	35
School Personal Data Advice and Guidance .....	36
School Policy – Online Safety Group Terms of Reference.....	46
Glossary of Terms .....	51



## Introduction

Policy has been underpinned from guidance from the following organisations

### SWGfL/UK Safer Internet Centre

SWGfL, along with partners Childnet and IWF, launched the UK Safer Internet Centre (UKSIC) in January 2011 as part of the European Commission's Safer Internet Programme. SWGfL is a founding member of UKCIS (UK Council for Internet Safety).

### 360 degree safe Online Safety Self Review Tool

360 degree safe is an online, interactive self review tool which allows our school to review our online safety policy and practice. [360safe.org.uk](http://360safe.org.uk).

The Online safety Policy will link with

- child protection/safeguarding policy
- behaviour and anti-bullying policies.
- KCSIE

Consultation in the production of this policy involved:

- Curriculum Governor
- Computing Lead/ SLT
- Parents
- Head teacher DSL
- Business manager
- EDAC Solutions Education Ltd –An educational specialist ICT support partner

This group formed the **Online Safety Group**





# Online Safety Policy

## Penketh Primary School



## Development/Monitoring/Review of this Policy

This online safety policy has been developed by a working group made up of:

- Curriculum and parent Governor James Parr
- Safeguarding Governor Rob Hindley
- Computing Lead/ SLT Gill Clarke
- Head teacher DSL Rebecca Kayll
- Business manager Marie Darlington
- EDAC Solutions Education Ltd –An educational specialist ICT support partner Nigel Spencer

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:	<i>Dec 2021</i>
Online Safety group – Business Manager Computing Lead Head teacher Nigel Spencer- Edac	<i>Nov 21 Review Nov 2022</i>
The implementation of this online safety policy will be monitored by the:	<i>DSL Rebecca Kayll Deputy DSL Phil Towey Computing Lead Becki Williams</i>
Monitoring will take place at regular intervals:	<i>Annually or following guidance updates</i>
The Governing Body will receive a report on the implementation of the online safety policy generated by the senior leadership team (which will include anonymous details of online safety incidents) at regular intervals:	<i>Termly as part of the safeguarding Governor meeting</i>
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:	<i>Nov 2022</i>
Should serious online safety incidents take place, the following external persons/agencies should be informed:	<i>LA Safeguarding Officer, LADO Police</i>

The school will monitor the impact of the policy using:

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

## Scope of the Policy

This policy applies to all members of Penketh Primary (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 Penketh Primary 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 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*:

### 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 Committee has taken on the role of Online Safety Governor : James Parr and Safeguarding Governor Rob Hindley. The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Co-ordinator
- 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 Mrs Rebecca Kayll 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 Mrs Gill Clarke
- 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 Warrington Local Authority and WPAT/other relevant body disciplinary procedures).
- The Headteacher and 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 and 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.
- Online Safety Lead Mrs Gill Clarke

- DSL Mrs Rebecca Kayll
- Deputy DSL Mr Phil Towey
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead.

**Online Safety Lead** : Miss Becki Williams

**DSL** Mrs Rebecca Kayll and **Deputy DSL** Mr Phil Towey

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

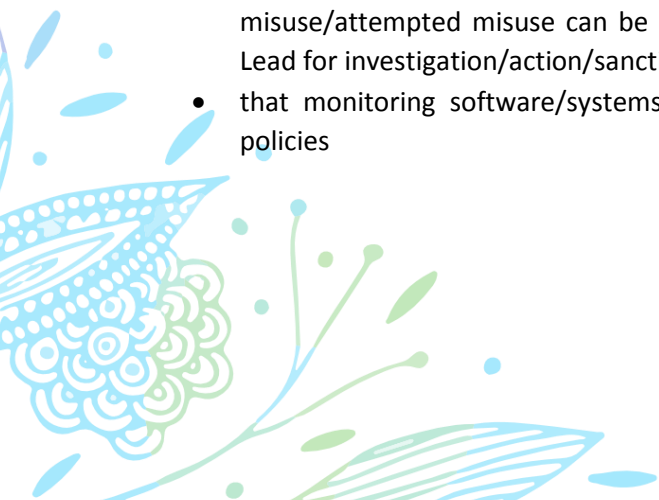
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Warrington Local Authority/WPAT/relevant body
- liaises with school technical staff - EDAC
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meets regularly with Safeguarding and Online Safety Governor to discuss current issues, review incident logs and filtering/change control logs
- attends relevant meetings of Governors
- reports regularly to Senior Leadership Team
- Investigation/action/sanctions will be the responsibility of the Online Safety Lead in conjunction with Headteacher and Senior Leader/Designated Safeguarding Lead

### **Network Manager/Technical staff**

Penketh Primary school has a managed ICT service provided by an outside contractor EDAC, it is the responsibility of the school to ensure that the managed service provider carries out all the online safety measures below. Edac is fully aware of the school online safety policy and procedures.

Those with technical responsibilities are 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 Warrington Local Authority/WPAT/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
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher and Senior Leaders; Online Safety Lead for investigation/action/sanction
- that monitoring software/systems are implemented and updated as agreed in school/academy policies



## Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current *school* online safety policy and practices
- they have read, understood and signed the staff acceptable use policy/agreement (AUP/AUA)
- they report any suspected misuse or problem to the *Headteacher/Senior Leader/Online Safety Lead* for investigation/action/sanction
- all digital communications with students/pupils/parents/carers should be on a professional level *and only carried out using official school systems*
- online safety issues are embedded in all aspects of the curriculum and other activities
- students/pupils understand and follow the Online Safety Policy and acceptable use policies
- they monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches-‘IF IN DOUBT SCREEN GOES OUT’

## 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 the monitoring the Online Safety Policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Committee

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

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

## Students/Pupils:

- are responsible for using the school digital technology systems in accordance with the pupil acceptable use agreement



- 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, social media 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/Learning Platform and on-line student/pupil records
- their children's personal devices in the school/academy (where this is allowed) i.e residential

### 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. As a school we use EAware to support our delivery
- Key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
- 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. There are additional duties for schools under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet.
- Pupils 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.

### **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](http://www.swgfl.org.uk), [www.saferinternet.org.uk/](http://www.saferinternet.org.uk/), <http://www.childnet.com/parents-and-carers>

### **Education – The Wider Community**

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

- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide online safety information for the wider community
- Sharing their online safety expertise/good practice

### **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/academy online safety policy and acceptable use agreements.
- The Online Safety Lead 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/training sessions.
- 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 group involved in technology/online safety/health and safety /safeguarding. This may be offered in a number of ways:

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

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

Penketh has a managed ICT service provided by an outside contractor –**EDAC Solutions**. The managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school. The managed service provider is fully aware of the school online safety policy/acceptable use agreements.

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.

- 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/academy technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school/academy technical systems and devices.
- All users (at KS2 and above) will be provided with a username and secure password by Edac who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- The “master/administrator” passwords for the school systems, used by the Network Manager must also be available to the Headteacher or Online Safety Lead and Business Manager and kept in a secure place
- **EDAC Solutions** is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- WBC regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement. Our contracted technical support team will review information from WBC and alert as required.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed- Report to Mrs Clarke or Mrs Kayll as internet safety leads ).
- 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 devices are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of “guests” (e.g. trainee teachers, supply teachers, visitors) onto the school systems. A ticket will be issued to allow 24 hour access with a pin number, once the 24 hour is up the pin will no long be active

- An agreed policy is in place, an acceptable use agreement, regarding the extent of personal use that users (staff/students/pupils/community users) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place that forbids staff from downloading executable files and installing programmes on school devices without technical administration authorising

### Mobile Technologies (including BYOD/BYOT)

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

All users should understand that the primary purpose of the use mobile/personal devices in a school context is educational. The mobile technologies policy is consistent with and inter-related to other relevant school policies including but not limited to the safeguarding policy, behaviour policy, bullying policy, acceptable use policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school’s online safety education programme.

### Pupils are not allowed to bring their own devices into school to access the school internet or network

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

	School Devices			Personal Devices		
	School owned for single user	School owned for multiple users	Authorised device <sup>1</sup>	Student owned	Staff owned	Visitor owned
Allowed in school	✓	✓	✓	✗	✓	✓
Full network access	✓	✗	✗	✗	✗	✗
Internet only	✓	✓	✓	✗	✓	✗
No network access		✓	✓	✓	✓	✓

acceptable use agreements indicate:

School owned/provided devices:

- Who they will be allocated to
- Where, when and how their use is allowed – times/places/in school/out of school
- If personal use is allowed
- Levels of access to networks/internet (as above)
- Management of devices/installation of apps/changing of settings/monitoring
- Network/broadband capacity
- Technical support
- Filtering of devices

<sup>1</sup> Authorised device – purchased by the pupil/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

- Access to cloud services
- Data Protection
- Taking/storage/use of images
- Exit processes – what happens to devices/software/apps/stored data if user leaves the school
- Liability for damage
- Staff training

#### **Personal devices:**

- Which users are allowed to use personal mobile devices in school (staff/visitors)
- Restrictions on where, when and how they may be used in school
- Storage
- Whether staff will be allowed to use personal devices for school business
- Levels of access to networks/internet (as above)
- Network/broadband capacity
- Technical support (this may be a clear statement that no technical support is available)
- Filtering of the internet connection to these devices
- Data Protection
- The right to take, examine and search users devices in the case of misuse (England only) – N.B. this must also be included in the Behaviour Policy.
- Taking/storage/use of images
- Liability for loss/damage or malfunction following access to the network (likely to be a disclaimer about school responsibility).
- Identification/labelling of personal devices
- How visitors will be informed about school requirements
- How education about the safe and responsible use of mobile devices is included in the school online safety education programmes.

#### **Use of digital and video images**

- When using digital images, staff should inform and educate students/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 students/pupils are published on the school website/social media/local press
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is 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 students/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 students/pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupil's work can only be published with the permission of the student/pupil and parents or carers.

### **Data Protection**

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

The school has:

- **a Data Protection Policy**
- IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring fenced from systems accessible in the classroom/to learners
- it has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed by EDAC Solutions
- it understands how to share data lawfully and safely with other relevant data controllers.
- it [reports any relevant breaches to the Information Commissioner](#) within 72hrs of becoming aware of the breach in accordance with UK data protection law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.
- We have a Freedom of Information Policy which sets out how it will deal with FOI requests.
- all staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.

When personal data is stored on any mobile device or removable media the:

- data must be encrypted and password protected.
- device must be password protected.
- device must be protected by up to date virus and malware checking software
- data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

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
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understand their rights and know how to handle a request whether verbal or written. Know who to pass it to in the school
- where personal data is stored or transferred on mobile or other devices (including USBs) these must be encrypted and password protected.
- will not transfer any school personal data to personal devices except as in line with school policy

- access personal data sources and records 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

## 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:

	Not allowed	Staff & other adults			Students/Pupils				
		Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
<b>Communication Technologies</b>									
Mobile phones may be brought to the school		✓						✓Y6	
Use of mobile phones in lessons	✓				✓				
Use of mobile phones in social time			✓		✓				
Taking photos on mobile phones/cameras	✓				✓				
Use of other mobile devices e.g. tablets, gaming devices			✓		✓				
Use of personal email addresses in school, or on academy network (access personal email but not to send school related)			✓		✓				
Use of school email for personal emails	✓				✓				
Use of messaging apps in social time			✓		✓				
Use of social media			✓		✓				
Use of blogs			✓		✓				

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

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.

- Users must immediately report, to the nominated person – 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 at KS1 and KS2 and above will be provided with individual school email addresses for educational use.
- Students/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, WPAT or Warrington local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

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

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

School staff should ensure that:

- No reference should be made in social media to students/pupils, parents/carers or school/academy 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 WPAT
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official school or WPAT 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
- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under school/academy disciplinary procedures



### Personal Use:

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

### Monitoring of Public Social Media:

- As part of active social media engagement, it is considered good practice to 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

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

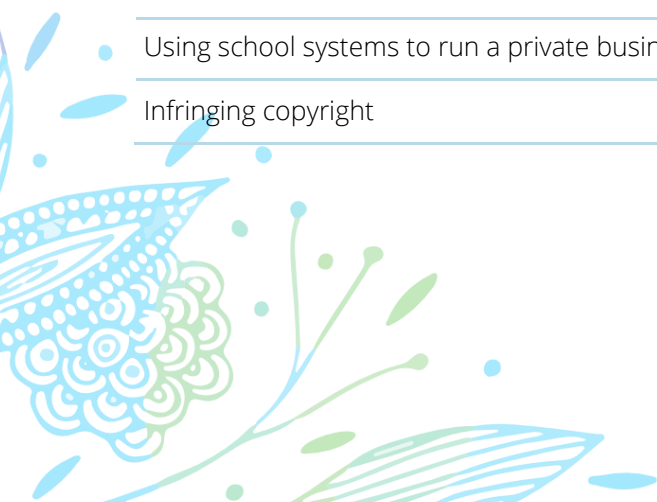
### Dealing with unsuitable/inappropriate activities

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

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

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978  N.B. Schools/academies should refer to guidance about dealing with self-generated images/sexting – <a href="#">UKSIC Responding to and managing sexting incidents</a> and <a href="#">UKCIS – Sexting in schools and colleges</a>					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X

on, material, remarks, proposals or comments that contain or relate to:	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Activities that might be classed as cyber-crime under the Computer Misuse Act:						
	<ul style="list-style-type: none"> <li>• Gaining unauthorised access to school networks, data and files, through the use of computers/devices</li> <li>• Creating or propagating computer viruses or other harmful files</li> <li>• Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)</li> <li>• Disable/Impair/Disrupt network functionality through the use of computers/devices</li> <li>• Using penetration testing equipment (without relevant permission)</li> </ul>					X
Under the Cyber-Prevent agenda the National Crime Agency has a remit to prevent young people becoming involved in cyber-crime and harness their activity in positive ways – further information <a href="#">here</a>						
	Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school/academy				X	
	Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				X	
	Using school systems to run a private business				X	
	Infringing copyright				X	



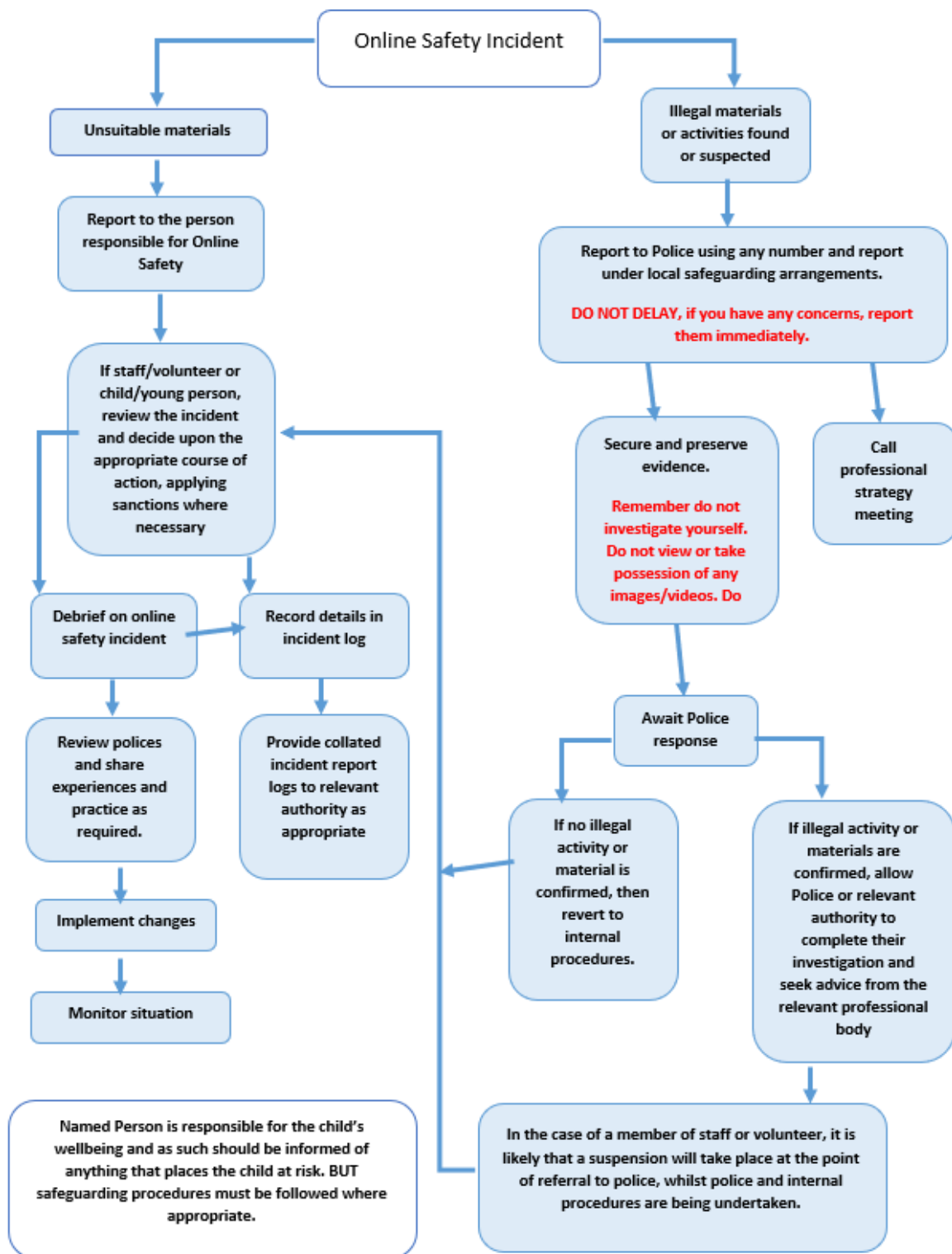
## Responding to incidents of misuse

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.**





## 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 WPAT and Warrington Local Authority or national/local organisation (as relevant).
  - Police involvement and/or action
- **If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
  - incidents of ‘grooming’ behaviour
  - the sending of obscene materials to a child
  - adult material which potentially breaches the Obscene Publications Act
  - criminally racist material
  - promotion of terrorism or extremism
  - offences under the Computer Misuse Act (see User Actions chart above)
  - 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.



# Appendix

## Appendices

Penketh Primary School .....	0
Online Safety Policy .....	0
Contents.....	1
<b>Introduction</b> .....	2
<b>Development/Monitoring/Review of this Policy</b> .....	4
Roles and Responsibilities .....	5
<b>Policy Statements</b> .....	8
<b>Communications</b> .....	14
<b>Dealing with unsuitable/inappropriate activities</b> .....	16
Responding to incidents of misuse .....	18
<b>Illegal Incidents</b> .....	18
Other Incidents .....	20
School actions & sanctions.....	<b>Error! Bookmark not defined.</b>
Appendix.....	21
Pupil Acceptable Use Agreement – for older students/pupils .....	22
Pupil Acceptable Use Policy Agreement – for younger pupils (Foundation/KS1) .....	25
Parent/Carer Acceptable Use Agreement.....	26
Staff (and Volunteer) Acceptable Use Policy Agreement Template .....	29
Acceptable Use Agreement for Community Users .....	<b>Error! Bookmark not defined.</b>
Responding to incidents of misuse – flow chart.....	32
Record of reviewing devices/internet sites (responding to incidents of misuse) .....	33
Reporting Log.....	34
Training Needs Audit Log.....	35
School Technical Security Policy (including filtering and passwords) .....	<b>Error! Bookmark not defined.</b>
School/academy Personal Data Advice and Guidance .....	36
School/academy policy template: Electronic Devices - Searching & Deletion.....	<b>Error! Bookmark not defined.</b>
Mobile Technologies Policy Template (inc. BYOD/BYOT).....	<b>Error! Bookmark not defined.</b>
Social Media Policy Template.....	<b>Error! Bookmark not defined.</b>
School Policy – Online Safety Group Terms of Reference.....	46
Legislation.....	47
Glossary of Terms.....	51



## Pupil Acceptable Use Agreement – for older students/pupils

### School policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe access to these digital technologies.

### This acceptable use agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

### Acceptable Use Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

### For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and **take an adult with me.**
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

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

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for anything other than the activity directed by my class teacher

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

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

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

- I will only use my own personal devices (mobile phones/USB devices etc.) in school if I have permission. I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will not access any social media sites

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

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

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

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

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.





## Pupil Acceptable Use Agreement Form

This form relates to the pupil acceptable use agreement; to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I use my own equipment out of the school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, VLE, website etc.

Name of Student/Pupil: .....

Group/Class: .....

Signed: .....

Date: .....

## Parent/Carer Countersignature

Name of parent/carers .....

Signed: .....

Date: .....



## Pupil Acceptable Use Policy Agreement – for younger pupils (Foundation/KS1)

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers/tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of computers/tablets and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer/tablet

Signed (child): .....

Date: .....

Signed (parent): .....

Date: .....



## Parent/Carer Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

### This acceptable use policy is intended to ensure:

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

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the pupil acceptable use agreement is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.

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

### Permission Form

Parent/Carers Name: .....

Student/Pupil Name: .....

As the parent/carers of the above pupils, I give permission for my son/daughter to have access to the internet and to ICT systems at school.

#### Either: (KS2 and above)

I know that my son/daughter has signed an acceptable use agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

#### Or: (KS1)

I understand that the school has discussed the acceptable use agreement with my son/daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

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

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

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

As the school/academy is collecting personal data by issuing this form, it should inform parents/carers as to:

This form (electronic or printed)
Who will have access to this form.
Where this form will be stored.
How long this form will be stored for.
How this form will be destroyed.

Signed: .....

Date: .....

### 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. Where an image is publicly shared by any means, only your child's first name will be used.

The school will comply with the Data Protection Act and request parent's/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 is 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.

Parents/carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents/carers to agree.

As the school/academy is collecting personal data by issuing this form, it should inform parents/carers as to:

This form (electronic or printed)	The images
Who will have access to this form.	Where the images may be published. Such as; Twitter, Facebook, the school/academy website, local press, etc. (see relevant section of form below)
Where this form will be stored.	Who will have access to the images.
How long this form will be stored for.	Where the images will be stored.
How this form will be destroyed.	How long the images will be stored for.
	How the images will be destroyed.
	How a request for deletion of the images can be made.

## Digital/Video Images Permission Form

Parent/Carers Name:.....Student/Pupil Name:.....

As the parent/carer of the above student/pupil, I agree to the school taking digital/video images of my child/children.	Yes/No
I agree to these images being used:	
<ul style="list-style-type: none"> <li>to support learning activities.</li> </ul>	Yes/No
<ul style="list-style-type: none"> <li>in publicity that reasonably celebrates success and promotes the work of the school.</li> </ul>	Yes/No
Insert statements here that explicitly detail where images are published by the school/academy	Yes/No
I agree that if I take digital or video images at, or of school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.	Yes/No

Signed: .....

Date: .....



## Staff (and Volunteer) Acceptable Use Policy Agreement Template

### School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools/academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

### This acceptable use policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school/academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

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

### Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students/pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

### For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school. (schools should amend this section in the light of their policies which relate to the personal use, by staff and volunteers, of school systems)
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

### I will be professional in my communications and actions when using school systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published

(e.g. on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.

- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with students/pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

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

- When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses
- I will not use personal email addresses on the school/academy ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school/academy policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school/academy policies.
- I will not disable or cause any damage to school/academy equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School/Academy/LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student/pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school/academy policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

### **When using the internet in my professional capacity or for school sanctioned personal use:**

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

### **I understand that I am responsible for my actions in and out of the school/academy:**

- I understand that this acceptable use policy applies not only to my work and use of school/academy digital technology equipment in school, but also applies to my use of school/academy systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school/academy

- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors/directors and/or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name: .....

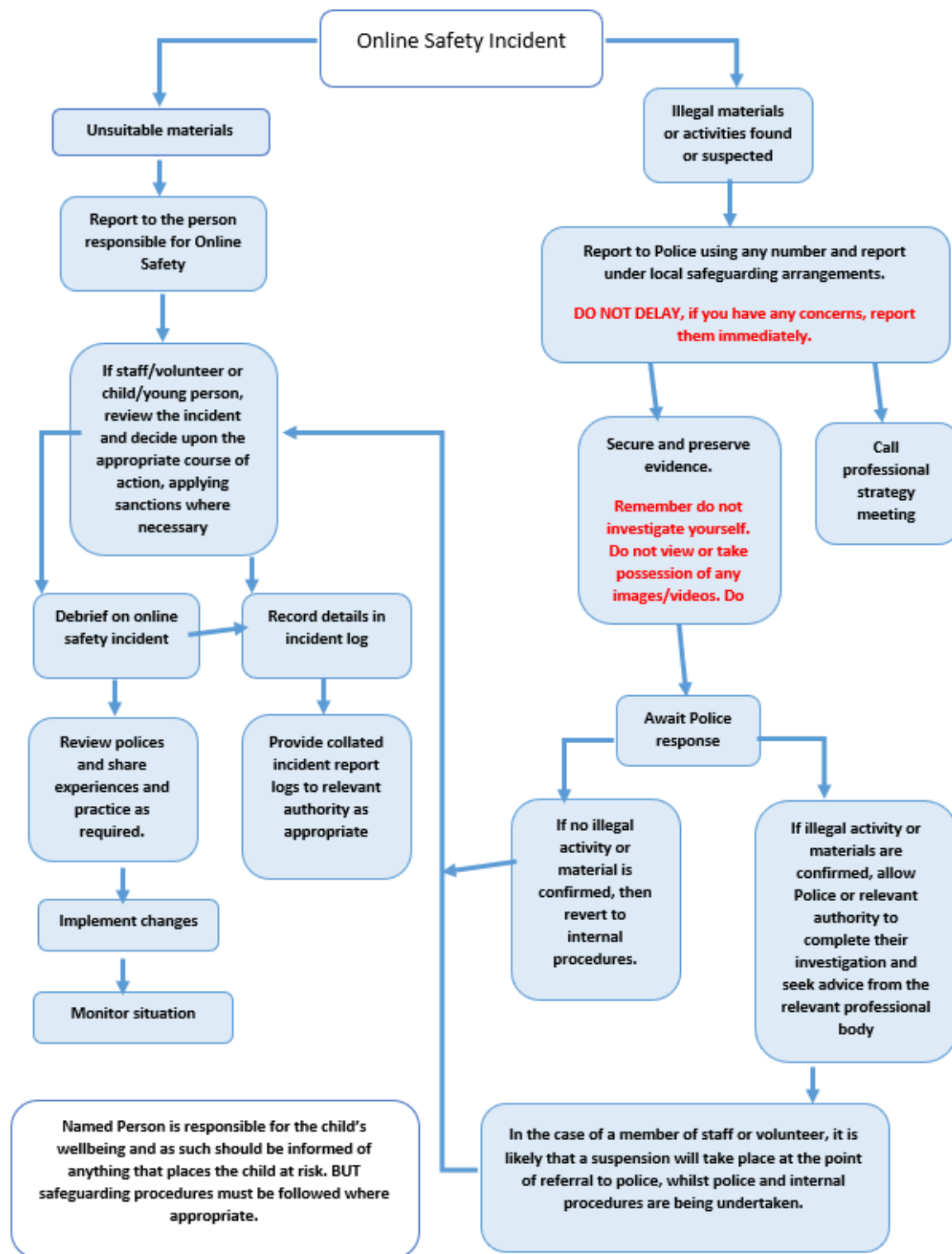
Signed: .....

Date: .....





# Responding to incidents of misuse – flow chart



# Record of reviewing devices/internet sites (responding to incidents of misuse)

Group: .....

Date: .....

Reason for investigation: .....

.....

.....

**Details of first reviewing person**

Name: .....

Position: .....

Signature: .....

**Details of second reviewing person**

Name: .....

Position: .....

Signature: .....

**Name and location of computer used for review (for web sites)**

.....

.....

Web site(s) address/device	Reason for concern

**Conclusion and Action proposed or taken**




# Reporting Log

Group: .....

Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		

# Training Needs Audit Log

Group: .....

Relevant training the last 12 months	Identified Training Need	To be met by	Cost	Review Date

# School Personal Data Advice and Guidance

## Data Protection Law – A Legislative Context

With effect from 25th May 2018, the data protection arrangements for the UK changed following the implementation of the European Union General Data Protection Regulation (GDPR). This represented a significant shift in legislation and in conjunction with the Data Protection Act 2018 replaced the Data Protection Act 1998.

GDPR - As a European Regulation, the GDPR has direct effect in UK law and automatically applies in the UK until we leave the EU (or until the end of any agreed transition period, if we leave with a deal). After this date, it will form part of UK law under the European Union (Withdrawal) Act 2018, with some technical changes to make it work effectively in a UK context.

Data Protection Act 2018 – this Act sits alongside the GDPR, and tailors how the GDPR applies in the UK and provides the UK-specific details such as; how to handle education and safeguarding information.

No Deal Brexit -The Information Commissioner advises that in the event of a no- deal Brexit it is anticipated that the Government of the day will pass legislation to incorporate GDPR into UK law alongside the DPA 2018. Unless your school/academy receives personal data from contacts in the EU there will be little change save to update references to the effective legislation in privacy notices etc.

In this document the term “Data Protection Law” refers to the legislation applicable to data protection and privacy as applicable in the UK from time to time.

## Does the Data Protection Law apply to schools?

In short, yes. Any natural or legal person, public authority, agency or other body which processes personal data is considered a ‘data controller’.

A school/academy is, for the purposes of the Data Protection Law, a “public body” and further processes the **personal data** of numerous **data subjects** on a daily basis.

Personal data is information that relates to an identified or identifiable living individual (a data subject).

Guidance for schools/academies is available on the [Information Commissioner’s Office](#) (ICO) website including information about the Data Protection Law.

The ICO’s powers are wide ranging in the event of non-compliance and schools/academies must be aware of the huge impact that a fine or investigation will have on finances and also in the wider community for example in terms of trust.

The Data Protection Law sets out that a data controller must ensure that personal data shall be:

- a) processed lawfully, fairly and in a transparent manner in relation to data subjects;
- b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes

for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the Data Protection Law in order to safeguard the rights and freedoms of data subjects; and

- f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

These principles of the Data Protection Law drive the need for the school/academy to put in place appropriate **privacy notices** (to give a data subject information about the personal data processing activities, **legal basis of processing** and **data subject rights**) and policies (such as for reporting a breach, managing a data subject access request, training, retention etc.) to demonstrate compliance.

## Data Mapping to identify personal data, data subjects and processing activities

The school/academy and its employees will collect and/ or process a wide range of information concerning numerous data subjects and some of this information will include personal data. Further, the school/academy may need to share some personal data with third parties. To be able to demonstrate and plan compliance and it is important that the school/academy has a **data map** of these activities; it can then make sure that the correct privacy notices are provided, put in place **security measures** to keep the personal data secure and other steps to avoid **breach** and also put in place data processing agreements with the third parties.

The data map should identify what personal data held in digital format or on paper records in a school/ academy, where it is stored, why it is processed and how long it is retained.

In a typical data map for a school/academy the data subjects and personal data will include, but is not limited to:

- Parents, legal guardians, governors – and personal data of names, addresses, contact details
- Learners - curricular / academic data e.g. class lists, learner progress records, reports, references, contact details, health and SEN reports
- Staff and contractors - professional records e.g. employment history, taxation and national insurance records, appraisal records and references, health records

Some types of personal data are designated as '**special category**' being personal data;

"revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation"

This should be identified separately and to lawfully process special category data, you must identify both a [lawful basis](#) and a [separate condition for processing special category data](#). You should decide and document this before you start processing the data.

The school/academy will need to identify appropriate lawful process criteria for each type of personal data and if this is not possible such activities should be discontinued. The lawful processing criteria can be summarised as:

- |                       |   |
|-----------------------|---|
| (a) Consent:          | the data subject has given clear consent for you to process their personal data for a specific purpose (see below for further guidance) |
| (b) Contract:         | the processing is necessary for a contract you have with the data subject   |
| (c) Legal obligation: | the processing is necessary for you to comply with the law (not including contractual obligations).                                     |
| (d) Vital interests:  | the processing is necessary to protect someone's life.  |

- (e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- (f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks) Please also be aware that these criteria must be supported by a written legitimate interest assessment.

No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the data subject.

Several of the lawful purpose criteria may relate to a particular specified purpose – a legal obligation, a contract with the individual, protecting someone's vital interests, or performing your public tasks. If you are processing for these purposes then the appropriate lawful basis may well be obvious, so it is helpful to consider these first.

As a public authority, and if you can demonstrate that the processing is to perform your tasks as set down in UK law, then you are able to use the public task basis. If not, you may still be able to consider consent or legitimate interests in some cases, depending on the nature of the processing and your relationship with the data subject. There is no absolute ban on public authorities using consent or legitimate interests as their lawful basis, but the Data Protection law does restrict public authorities' use of these two criteria.

The majority of processing of personal data conducted by public authorities will fall within Article 6(1)(e) GDPR, that "*processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller*" however careful consideration must be given to any processing, especially in more novel areas. As you can see, consent is just one of several possible lawful processing criteria.

Consent has changed as a result of the GDPR and is now defined as: "in relation to the processing of personal data relating to an individual, means a freely given, specific, informed and unambiguous indication of the individual's wishes by which the individual, by a statement or by a clear affirmative action, signifies agreement to the processing of the personal data"

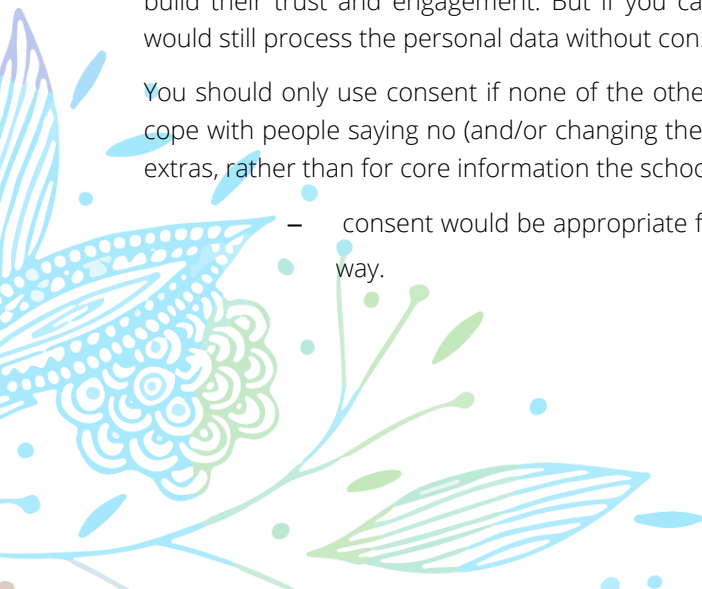
This means that where a school/academy is relying on consent as the basis for processing personal data that consent has to be clear, meaning that pre-ticked boxes, opt-out or implied consent are no longer suitable. The GDPR does not specify an age of consent for general processing but schools/academies should consider the capacity of pupils to freely give their informed consent.

The Information Commissioner's Office (ICO) gives clear advice on when it's appropriate to [use consent](#) as a lawful base. It states:

"Consent is appropriate if you can offer people real choice and control over how you use their data and want to build their trust and engagement. But if you cannot offer a genuine choice, consent is not appropriate. If you would still process the personal data without consent, asking for consent is misleading and inherently unfair."

You should only use consent if none of the other lawful bases is appropriate. If you do so, you must be able to cope with people saying no (and/or changing their minds), so it's important that you only use consent for optional extras, rather than for core information the school requires in order to function. Examples;

- consent would be appropriate for considering whether a child's photo could be published in any way.



- if your school or academy requires learner details to be stored in an MIS, it would not be appropriate to rely on consent if the learner cannot opt out of this. In this case, you could apply the public task lawful base.

## Content of Privacy Notices

Privacy Notices are a key compliance requirement as they ensure that each data subject is aware of the following points when data is collected/ processed by a data controller:

- Who the controller of the personal data is
- What personal data is being processed and the lawful purpose of this processing
- where and how the personal data was sourced
- to whom the personal data may be disclosed
- how long the personal data may be retained
- data subject's rights and how to exercise them or make a complaint

In order to comply with the fair processing requirements in data protection law, the school/academy will inform parents/carers of all learners of the data they collect, process and hold on the learners, the purposes for which the data is held and the third parties (e.g. LA etc.) to whom it may be passed. This privacy notice will be passed to parents/carers for example in the prospectus, newsletters, reports or a specific letter / communication or you could publish it on your website and keep it updated there. Parents/carers of young people who are new to the school/academy will be provided with the privacy notice through an appropriate mechanism.

In some circumstances you may also require privacy notices for children / learners as data subjects as children have the same rights as adults over their personal data. These include the rights to access their personal data; request rectification; object to processing and have their personal data erased. The policies that explain this should be clear and age appropriate.

## Data subject's right of access

Data subjects have a number of rights in connection with their personal data. They have the right:

- to be informed – Privacy Notices
- of access – Subject Access Requests
- to rectification – correcting errors
- to erasure – deletion of data when there is no compelling reason to keep it
- to restrict processing – blocking or suppression of processing
- to portability – unlikely to be used in a school/academy context
- to object – objection based on grounds pertaining to their situation
- related to automated decision making, including profiling

Several of these could impact schools and academies, such as the right of access. You need to put procedures in place to deal with [Subject Access Requests](#). These are written or verbal requests to see all or a part of the personal data held by the Controller in connection with the data subject. Controllers normally have 1 calendar month to provide the information, unless the case is unusually complex in which case an extension can be obtained.

A school/academy must not disclose personal data even if requested in a Subject Access Request;

- if doing so would cause serious harm to the individual
- child abuse data
- adoption records
- statements of special educational needs



Your school or academy must provide the information free of charge. However, if the request is clearly unfounded or excessive – and especially if this is a repeat request – you may charge a reasonable fee.

## Breaches and how to manage a breach

Recent publicity about data breaches suffered by organisations and individuals continues to make the area of personal data protection a current and high profile issue for schools, academies and other organisations. It is important that the school/academy has a clear and well understood personal data handling policy in order to minimise the risk of personal data breaches.

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

A breach may arise from a theft, a deliberate attack on your systems, the unauthorised or malicious use of personal data by a member of staff, accidental loss, or equipment failure. In addition:

- no school/academy or individual would want to be the cause of a data breach, particularly as the impact of data loss on individuals can be severe, put individuals at risk and affect personal, professional or organisational reputation
- schools/academies are “data rich” and the introduction of electronic storage and transmission of data has created additional potential for the loss of data
- the school/academy will want to avoid the criticism and negative publicity that could be generated by any personal data breach

Schools / academies have always held personal data on the learners in their care, and increasingly this data is held digitally and accessible not just in school/academy but also from remote locations. It is important to stress that the Data Protection Laws apply to all forms of personal data, regardless of whether it is held on paper or in electronic format. However, as it is part of an overall online safety policy template, this document will place particular emphasis on data which is held or transferred digitally.

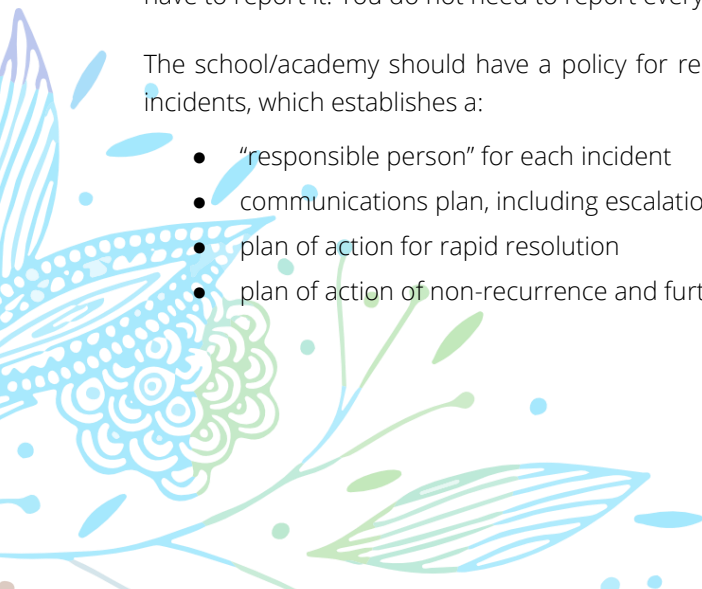
Schools / Academies will need to carefully review their policy, in the light of pertinent Local Authority regulations and guidance and changes in legislation.

All significant [data protection incidents must be reported](#) through the DPO to the Information Commissioner’s Office based upon the local incident handling policy and communication plan. The new laws require that this notification should take place within 72 hours of the breach being detected, where feasible.

If you experience a personal data breach you need to consider whether this poses a risk to people. You need to consider the likelihood and severity of any risk to people’s rights and freedoms, following the breach. When you’ve made this assessment, if it’s likely there will be a risk then you must notify the ICO; if it’s unlikely then you don’t have to report it. You do not need to report every breach to the ICO.

The school/academy should have a policy for reporting, logging, managing and recovering from information risk incidents, which establishes a:

- “responsible person” for each incident
- communications plan, including escalation procedure
- plan of action for rapid resolution
- plan of action of non-recurrence and further awareness raising



## Privacy by Design and Data Protection Impact Assessments (DPIA)

Data Protection Impact Assessments (DPIA) identify and address privacy risks early on in any project so that you can mitigate them before the project goes live.

DPIAs should be carried out by Data Managers (where relevant) under the support and guidance of the DPO. Ideally you should conduct a DPIA before processing activity starts. However, some may need to be retrospective in the early stages of compliance activity.

The risk assessment will involve:

- recognising the risks that are present
- judging the level of the risks (both the likelihood and consequences)
- prioritising the risks.

According to the ICO a DPIA should contain:

- a description of the processing operations and the purpose
- an assessment of the necessity and proportionality of the processing in relation to the purpose
- an assessment of the risks to individuals
- the measures in place to address risk, including security and to demonstrate that you comply.

Or more simply and fully:

- who did you talk to about this?
- what is going to happen with the data and how – collection, storage, usage, disposal
- how much personal data will be handled (number of subjects)
- why you need use personal data in this way
- what personal data (including if it's in a 'special category') are you using
- at what points could the data become vulnerable to a breach (loss, stolen, malicious)
- what the risks are to the rights of the individuals if the data was breached
- what are you going to do in order to reduce the risks of data loss and prove you are compliant with the law.

DPIA is an ongoing process and should be re-visited at least annually to verify that nothing has changed since the processing activity started.

## Secure storage of and access to data

The school/academy should ensure that systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

[Good practice](#) suggests that all users will use strong passwords made up from a combination of simpler words. User passwords must never be shared.

Personal data may only be accessed on machines that are securely protected. Any device that can be used to access personal data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data should only be stored on school/academy equipment. Private equipment (i.e. owned by the users) must not be used for the storage of school/academy personal data.

When personal data is stored on any portable computer system, USB 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 once it has been transferred or its use is complete.

The school/academy will need to set its own policy as to whether data storage on removal media is allowed, even if encrypted. Some organisations do not allow storage of personal data on removable devices.

The school/academy should have a clear policy and procedures for the automatic backing up, accessing and restoring of all data held on school/academy systems, including off-site backups.

The school/academy should have clear policy and procedures for the use of “Cloud Based Storage Systems” (for example Dropbox, Microsoft 365, Google Drive) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school/academy will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data.

As a Data Controller, the school/academy is responsible for the security of any data passed to a “third party”. Specific data processing clauses must be included in all contracts where personal data is likely to be passed to a third party.

All paper based personal data must be held in lockable storage, whether on or off site.

## Secure transfer of data and access out of school

The school/academy recognises that personal data may be accessed by users out of school/academy or transferred to the local authority or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school/academy or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school/academy
- When restricted or protected personal data is required by an authorised user from outside the organisation’s premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority (if relevant) in this event.

## Disposal of personal data

The school/academy should implement a document retention schedule that defines the length of time personal data is held before secure destruction. The Information and Records Management Society [Toolkit for schools](#) provides support for this process. The school/academy must ensure the safe destruction of personal data when it is no longer required.

The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely disposed of, and other media must be shredded, incinerated or otherwise disintegrated.

A Destruction Log should be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.

## **Demonstrating Compliance - Audit Logging / Reporting / Incident Handling**

Organisations are required to keep records of processing activity. The data map referred to above will assist here. Records must include:

- the name and contact details of the data controller
- where applicable, the name and contact details of the joint controller and data protection officer
- the purpose of the processing
- to whom the data has been/will be disclosed
- description of data subject and personal data
- where relevant the countries it has been transferred to
- under which condition for processing the personal data has been collected
- under what lawful basis processing is being carried out
- where necessary, how it is retained and destroyed
- a general description of the technical and organisational security measures.

Clearly, in order to maintain these records good auditing processes must be followed, both at the start of the exercise and on-going throughout the lifetime of the requirement. Therefore, audit logs will need to be kept to:

- provide evidence of the processing activity and the DPIA
- record where, why, how and to whom personal data has been shared
- log the disposal and destruction of the personal data
- enable the school/academy to target training at the most at-risk data
- record any breaches that impact on the personal data

## **Fee**

The school/academy should pay the relevant annual fee to the Information Commissioner's Office (ICO). Failure to renew may render the school/academy to a penalty in addition to other fines possible under the Data Protection Law.

## **Responsibilities**

Every maintained school/academy is required to appoint a Data Protection Officer as a core function of 'the business'

The Data Protection Officer (DPO) can be internally or externally appointed.

### **They must have:**

- expert knowledge
- timely and proper involvement in all issues relating to data protection
- the necessary resources to fulfil the role
- access to the necessary personal data processing operations
- a direct reporting route to the highest management level



#### **The data controller must:**

- not give the DPO instructions regarding the performance of tasks
- ensure that the DPO does not perform a duty or role that would lead to a conflict of interests
- not dismiss or penalise the DPO for performing the tasks required of them

#### **As a minimum a Data Protection Officer must:**

- inform, as necessary, the controller, a processor or an employee of their obligations under the data protection laws
- provide advice on a data protection impact assessment
- co-operate with the Information Commissioner
- act as the contact point for the Information Commissioner
- monitor compliance with policies of the controller in relation to the protection of personal data
- monitor compliance by the controller with Data Protection Law

The school/academy may also wish to appoint a Data Manager. Schools/academies are encouraged to separate this role from that of Data Protection Officer, where possible. This person will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the school's / academy's information risk policy and risk assessment
- oversee the System Controllers

The school/academy may also wish to appoint System Controllers for the various types of data being held (e.g. learner information / staff information / assessment data etc.). System Controllers will manage and address risks to the information and will understand:

- what information is held, for how long and for what purpose
- how information has been amended or added to over time, and
- who has access to the data and why.

Everyone in the school/academy has the responsibility of handling protected or sensitive data in a safe and secure manner.

Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor (either in the school/academy or elsewhere if on school/academy business).

### **Training & awareness**

All staff must receive data handling awareness / data protection training and will be made aware of their responsibilities. This should be undertaken regularly. You can do this through:

- Induction training for new staff
- Staff meetings / briefings / INSET
- Day to day support and guidance from System Controllers

### **Freedom of Information Act**

All schools / academies must have a Freedom of Information Policy which sets out how it will deal with FOI requests. FOI aims to increase transparency and accountability in public sector organisations as part of a healthy democratic process. Whilst FOI requests are submitted by an individual, the issue is for the school/academy to consider whether the requested information should be released into the public domain. FOI links to Data

Protection Law whenever a request includes personal data. Good advice would encourage the school/academy to:

- delegate to the Headteacher day-to-day responsibility for FOI policy and the provision of advice, guidance, publicity and interpretation of the school's/academy's policy
- consider designating an individual with responsibility for FOI, to provide a single point of reference, coordinate FOI and related policies and procedures, take a view on possibly sensitive areas and consider what information and training staff may need
- consider arrangements for overseeing access to information and delegation to the appropriate governing body
- proactively publish information with details of how it can be accessed through a Publication Scheme (see Model Publication Scheme below) and review this annually
- ensure that a well-managed records management and information system exists in order to comply with requests
- ensure a record of refusals and reasons for refusals is kept, allowing the school/academy to review its access policy on an annual basis

### Model Publication Scheme

The Information Commissioner's Office provides schools and organisations with a [model publication scheme](#) which they should complete. The school's / academy's publication scheme should be reviewed annually.

The ICO produce [guidance on the model publication scheme](#) for schools. This is designed to support schools / academies complete the [Guide to Information for Schools](#).

### Use of Biometric Information

Biometric information is special category data. The Protection of Freedoms Act 2012, included measures that affect schools/academies that use biometric recognition systems, such as fingerprint identification and facial scanning:

- For all pupils in schools/academies under 18, they must obtain the written consent of a parent before they take and process their child's biometric data
- They must treat the data with appropriate care and must comply with data protection principles as set out in the Data Protection Law
- They must provide alternative means for accessing services where a parent or pupil has refused consent

[New advice](#) to schools/academies makes it clear that they are not able to use pupils' biometric data without parental consent. Schools/academies may wish to incorporate the parental permission procedures into revised consent processes. (see [Appendix Parent / Carer Acceptable Use Agreement](#))

### Privacy and Electronic Communications

Schools/academies should be aware that they are subject to the Privacy and Electronic Communications Regulations in the operation of their websites.



# School Policy – Online Safety Group Terms of Reference

## 1. Purpose

To provide a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring the online safety policy including the impact of initiatives.

## 2. Membership

2.1. The online safety group will seek to include representation from all stakeholders.

The composition of the group should include

- SLT member/s
- Child Protection/Safeguarding officer DLS
- Teaching staff member
- Edac Solutions Technical support safety coordinator
- Governor
- Parent/Carer

2.2. Other people may be invited to attend the meetings at the request of the Chairperson on behalf of the committee to provide advice and assistance where necessary.

2.3. Committee members must declare a conflict of interest if any incidents being discussed directly involve themselves or members of their families.

2.4. Committee members must be aware that many issues discussed by this group could be of a sensitive or confidential nature

2.5. When individual members feel uncomfortable about what is being discussed they should be allowed to leave the meeting with steps being made by the other members to allow for these sensitivities

## 3. Chairperson

The Committee should select a suitable Chairperson from within the group. Their responsibilities include:

- Scheduling meetings and notifying committee members;
- Inviting other people to attend meetings when required by the committee;
- Guiding the meeting according to the agenda and time available;
- Ensuring all discussion items end with a decision, action or definite outcome;
- Making sure that notes are taken at the meetings and that these with any action points are distributed as necessary

## 4. Duration of Meetings

Meetings shall be held **termly** for a period of **1/2** hour(s). A special or extraordinary meeting may be called when and if deemed necessary.

## 5. Functions

These are to assist the Online Safety Lead (or other relevant person) with the following

- To keep up to date with new developments in the area of online safety
- To (at least) annually review and develop the online safety policy in line with new technologies and incidents
- To monitor the delivery and impact of the online safety policy
- To monitor the log of reported online safety incidents (anonymous) to inform future areas of teaching/learning/training.
- To co-ordinate consultation with the whole school/academy community to ensure stakeholders are up to date with information, training and/or developments in the area of online safety. This could be carried out through [add/delete as relevant]:
  - Staff meetings
  - Student/pupil forums (for advice and feedback)

- Governors meetings
- Surveys/questionnaires for students/pupils, parents/carers and staff
- Parents evenings
- Website/VLE/Newsletters
- Online safety events
- Internet Safety Day (annually held on the second Tuesday in February)
- Other methods
- To ensure that monitoring is carried out of Internet sites used across the school/academy
- To monitor filtering/change control logs (e.g. requests for blocking/uN.B.locking sites).
- To monitor the safe use of data across the school/academy
- To monitor incidents involving cyberbullying for staff and pupils

## 6. Amendments

The terms of reference shall be reviewed annually from the date of approval. They may be altered to meet the current needs of all committee members, by agreement of the majority

The above Terms of Reference for [Penketh Primary school](#) have been agreed

Signed by (SLT): .....

Date: .....

Date for review: .....





## Links to other organisations or documents

The following links may help those who are developing or reviewing a school online safety policy and creating their online safety provision:

### UK Safer Internet Centre

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

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

Childnet – <http://www.childnet-int.org/>

Professionals Online Safety Helpline - <http://www.saferinternet.org.uk/about/helpline>

Revenge Porn Helpline - <https://revengepornhelpline.org.uk/>

Internet Watch Foundation - <https://www.iwf.org.uk/>

Report Harmful Content - <https://reportharmfulcontent.com/>

### CEOP

CEOP - <http://ceop.police.uk/>

ThinkUKnow - <https://www.thinkuknow.co.uk/>

### Others

LGfL – [Online Safety Resources](#)

Kent – [Online Safety Resources page](#)

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

UK Council for Internet Safety (UKCIS) - <https://www.gov.uk/government/organisations/uk-council-for-internet-safety>

Netsmartz - <http://www.netsmartz.org/>

### Tools for Schools

Online Safety BOOST – <https://boost.swgfl.org.uk/>

360 Degree Safe – Online Safety self-review tool – <https://360safe.org.uk/>

360Data – online data protection self-review tool: [www.360data.org.uk](http://www.360data.org.uk)

SWGfL Test filtering - <http://testfiltering.com/>

UKCIS Digital Resilience Framework - <https://www.gov.uk/government/publications/digital-resilience-framework>

### Bullying/Online-bullying/Sexting/Sexual Harassment

Enable – European Anti Bullying programme and resources (UK coordination/participation through SWGfL & Diana Awards) - <http://enable.eun.org/>

SELMA – Hacking Hate - <https://selma.swgfl.co.uk>

Scottish Anti-Bullying Service, Respectme - <http://www.respectme.org.uk/>

Scottish Government - Better relationships, better learning, better behaviour -

<http://www.scotland.gov.uk/Publications/2013/03/7388>

DfE - Cyberbullying guidance -

[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/374850/Cyberbullying\\_Advice\\_for\\_Headteachers\\_and\\_School\\_Staff\\_121114.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf)

Childnet – Cyberbullying guidance and practical PSHE toolkit:

<http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit>  
[Childnet – Project deSHAME – Online Sexual Harrassment](#)  
[UKSIC – Sexting Resources](#)  
Anti-Bullying Network – <http://www.antibullying.net/cyberbullying1.htm>  
[Ditch the Label – Online Bullying Charity](#)  
[Diana Award – Anti-Bullying Campaign](#)

## **Social Networking**

Digizen – [Social Networking](#)  
UKSIC - [Safety Features on Social Networks](#)  
[Children’s Commissioner, TES and Schillings – Young peoples’ rights on social media](#)

## **Curriculum**

SWGfL Evolve - <https://projectevolve.co.uk>  
[UKCCIS – Education for a connected world framework](#)  
Teach Today – [www.teachtoday.eu/](http://www.teachtoday.eu/)  
Insafe - [Education Resources](#)

## **Data Protection**

[360data - free questionnaire and data protection self review tool](#)  
[ICO Guides for Education \(wide range of sector specific guides\)](#)  
[DfE advice on Cloud software services and the Data Protection Act](#)  
[IRMS - Records Management Toolkit for Schools](#)  
[NHS - Caldicott Principles \(information that must be released\)](#)  
[ICO Guidance on taking photos in schools](#)  
[Dotkumo - Best practice guide to using photos](#)

## **Professional Standards/Staff Training**

[DfE – Keeping Children Safe in Education](#)  
DfE - [Safer Working Practice for Adults who Work with Children and Young People](#)  
[Childnet – School Pack for Online Safety Awareness](#)  
[UK Safer Internet Centre Professionals Online Safety Helpline](#)

## **Infrastructure/Technical Support**

[UKSIC – Appropriate Filtering and Monitoring](#)  
[SWGfL Safety & Security Resources](#)  
Somerset - [Questions for Technical Support](#)  
NCA – [Guide to the Computer Misuse Act](#)  
NEN – [Advice and Guidance Notes](#)

## **Working with parents and carers**

[Online Safety BOOST Presentations - parent’s presentation](#)  
[Vodafone Digital Parents Magazine](#)  
[Childnet Webpages for Parents & Carers](#)

[Get Safe Online - resources for parents](#)

[Teach Today - resources for parents workshops/education](#)

[Internet Matters](#)

## **Prevent**

[Prevent Duty Guidance](#)

[Prevent for schools – teaching resources](#)

[NCA – Cyber Prevent](#)

Childnet – [Trust Me](#)

## **Research**

[Ofcom –Media Literacy Research](#)

Further links can be found at the end of the UKCIS [Education for a Connected World Framework](#)



## Glossary of Terms

<b>AUP/AUA</b>	Acceptable Use Policy/Agreement – see templates earlier in this document
<b>CEOP</b>	Child Exploitation and Online Protection Centre (part of National Crime Agency, UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
<b>CPD</b>	Continuous Professional Development
<b>FOSI</b>	Family Online Safety Institute
<b>ICO</b>	Information Commissioners Office
<b>ICT</b>	Information and Communications Technology
<b>INSET</b>	In Service Education and Training
<b>IP address</b>	The label that identifies each computer to other computers using the IP (internet protocol)
<b>ISP</b>	Internet Service Provider
<b>ISPA</b>	Internet Service Providers' Association
<b>IWF</b>	Internet Watch Foundation
<b>LA</b>	Local Authority
<b>LAN</b>	Local Area Network
<b>MAT</b>	Multi Academy Trust
<b>MIS</b>	Management Information System
<b>NEN</b>	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
<b>Ofcom</b>	Office of Communications (Independent communications sector regulator)
<b>SWGfL</b>	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
<b>TUK</b>	Think U Know – educational online safety programmes for schools, young people and parents.
<b>UKSIC</b>	UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.
<b>UKCIS</b>	UK Council for Internet Safety
<b>VLE</b>	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
<b>WAP</b>	Wireless Application Protocol

A more comprehensive glossary can be found at the end of the UKCIS [Education for a Connected World Framework](#)

