



# Gidea Park

PREPARATORY SCHOOL AND NURSERY

## E-Safety Policy

This policy applies to all pupils in school, including in the EYFS

January 2023

Reviewed	<i>Jan 2023</i>
Next review	<i>Jan 2024</i>
Revised by	<i>T Ward</i>

## 1. Overview and Scope of this policy

This policy applies to all members of the school (including staff, pupils, volunteers, parents/carers, visitors) who have access to the school's IT system.

Both this policy and the Acceptable Use Policy (for all staff, visitors and pupils), cover fixed and mobile internet devices provided by the school as well as all devices owned by pupils, staff, or visitors and brought onto school premises.

This policy applies primarily within school. However, it is important to note that the Education and Inspections Act 2006 empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school premises.

This is pertinent to incidents of cyber-bullying or other e-Safety incidents covered by this policy, which may take place outside of the school, but are possibly **linked to membership of the school**.

The school will deal with such incidents, and will impose sanctions when appropriate, within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-Safety behaviour which take place out of school.

## 2. References and Guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, [Keeping Children Safe in Education \(September 2022\)](#), and its advice for schools on:

- [Teaching online safety in schools](#)
- [Preventing and tackling bullying](#) and [cyber-bullying: advice for head teachers and school staff](#)
- [Relationships and sex education](#)
- [Searching, screening and confiscation](#)

It also refers to the Department's guidance on [protecting children from radicalisation](#).

This policy reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#) and the [Equality Act 2010](#).

In addition, it reflects the [Education Act 2011](#), which has given teachers stronger powers to tackle cyber-bullying.

ISI Handbook September 2020

### 3 Schedule for Development / Monitoring / Review

This E-Safety Policy was approved by the Senior Leadership Team	<i>January 2023</i>
Monitoring will take place at regular intervals	<i>Every year at minimum</i>
The e-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>January 2023</i>
The implementation of this Online Safety policy will be monitored by the	<i>Designated Safeguarding Lead ICT /e-Safety Co-Ordinator</i>
The Senior Leadership Team will receive a report on the implementation of the e-Safety Policy	<i>Every year</i>
Should serious online safety incidents take place, the following persons should be informed:	<i>Designated Safeguarding Lead, Mr C Douglas</i>
Should serious online safety incidents take place, they will be fully recorded	<i>In the incident log</i>
To monitor the impact of this policy surveys will be used	<i>Staff; pupils and parents/carers</i>

### 4. Related Policies

This policy, supported by the Acceptable Use Policy (for all staff, visitors and pupils) is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. It is linked to the following school policies:

- Child Protection and Safeguarding
- Code of Conduct
- Health and Safety
- Behaviour Management
- Anti-Bullying
- Acceptable Use Policy
- Photography
- Data Protection
- PSHRE

## 5. e-Safety Statement

### **The purpose of this policy is to:**

- Ensure the safety and wellbeing of children is protected when adults and pupils are using the internet, mobile devices or social media.
- Provide staff and volunteers with the overarching principles that guide our approach to e-Safety
- Ensure that, as a School, we operate in line with our values and within the law in terms of how we use online devices.

This policy applies to all staff, volunteers and pupils involved in Gidea Park Preparatory School and Nursery.

### **We believe that:**

- Children should never experience abuse of any kind
- Children should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times

### **We recognise that:**

- The online world provides everyone with unrivalled opportunities for enhanced learning and communication; however it can also present risk and challenges
- We have a duty to ensure that all children and adults involved in our School are protected from harm online
- We have a responsibility to help keep children safe online, whether or not they are using the School's network and devices
- All children, regardless of age, disability, gender, race, religion or belief, have the right to equal protection from all types of harm or abuse
- Working in partnership with children, their parents, carers and other agencies is essential in promoting young people's welfare and in helping them to be responsible in their approach to online safety.

At Gidea Park Preparatory School and Nursery our pupils are taught how to stay safe in this continually evolving online environment. They are also taught how to mitigate risks, including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking, abuse and radicalisation.

## 6. Roles and Responsibilities

### **a. Proprietors:**

The Proprietors are responsible for the approval of the e-Safety Policy and for reviewing the effectiveness of this policy. The Proprietor receives regular information about e-Safety: universal information; school specific information including as appropriate, incident and monitoring reports through regular governance meetings and reports.

**b. Head/Senior Leaders:**

- The Head has a duty of care for ensuring the safety (including e-Safety) of members of the school community, though the day-to-day responsibility for e-Safety may be delegated to the e-Safety Co-ordinator.
- The Head will ensure staff are aware of the school procedures and policies that should be followed in the event of the abuse or suspected breach of e-safety in connection to the school.
- The Head and members of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-Safety allegation being made against a member of staff (see flow chart on dealing with e-Safety incidents – included in a later section, page 16).
- The Head is responsible for ensuring that the e-Safety Co-ordinator and other relevant staff receive suitable training to enable them to carry out their e-Safety roles and to train other colleagues, as relevant.

**c. Designated Safeguarding Lead**

The DSL takes lead responsibility for monitoring incidents and handling sensitive issues (including Child Protection), in particular:

- Ensuring that any online safety issues or incidents are resolved and that concerns arising are properly addressed
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Liaising with other agencies and/or external services if necessary
- Is trained in Online Safety issues and is 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
  - cyber-bullying
  - preventing radicalisation

**d. e-Safety Co-ordinator:**

- Takes day-to-day responsibility for e-Safety issues and has a leading role in establishing and reviewing the school e-Safety policies/documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident taking place.
- Receives reports of e-Safety incidents and creates a log of incidents to inform future e-Safety developments.
- Ensures that they keep up to date with current e-Safety technical information, issues and guidance issued by relevant organisations (including the ISI, the Local Authority, CEOP, Childnet and the Local Safeguarding Partnership) in order to effectively carry out their e-Safety role and to inform and update others as relevant.

**e. IT Support (Rika Technologies)**

Rika Technologies have a key role in maintaining a safe technical infrastructure at the school and in keeping abreast with the rapid succession of technical developments. They are responsible for:

- Security of the school's hardware system and its electronic data
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a continuous basis
- Putting in place appropriate filtering and monitoring systems, such as Smoothwall, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Reporting inappropriate usage or content to the Head.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 2 ) and dealt with appropriately in line with this policy

This list is not intended to be exhaustive.

**f. Teaching and Support Staff** are responsible for ensuring that:

- they have an up to date awareness of e-Safety matters and of the current school e-Safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Agreement
- they report any suspected misuse or problem to the Head/e-Safety Co-ordinator for investigation/action
- all digital communications with pupils/parents/carers are on a professional level

- they implement this policy consistently and ensure that any online incidents, including cyber bullying, are logged and dealt with in accordance with school policy.
- pupils understand and follow the e-Safety and acceptable use policies
- they encourage a 'talking and listening' culture to address e-Safety issues which may arise

#### **g. Pupils:**

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy
- 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 cyber-bullying
- should understand the importance of adopting good e-Safety practice when using digital technologies out of school, and realise that the school's e-Safety Policy covers their actions out of school, **if related to their membership of the school**

#### **h. 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 both in and outside school. Parents and carers are responsible for:

- Ensuring their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 2 and 3)
- Endorsing and supporting the school's Pupil Acceptable Use Policy.
- Following guidelines on the appropriate use of digital and video images taken at school events.
- Notifying a member of staff or the head of any concerns or queries regarding this policy

The school will take every opportunity to help parents understand these issues through providing information via newsletters, website, parents' evenings, e-Safety Briefing sessions. In addition, useful resources include:

- What are the issues? - [UK Safer Internet Centre](#)
- Hot topics - [Childnet International](#)
- Parent factsheet - [Childnet International](#)

The school will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

#### **i. Visitors and members of the community**

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use as outlined in the Acceptable Use Policy.

## 7 Awareness and Training

### a. Staff/Volunteers: awareness and training

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:

- **All new staff** should receive online safety training as part of their induction programme, ensuring that they fully understand the school e-Safety Policy and Acceptable Use Agreements.
- **All teaching staff** should have access to a planned programme of formal online safety training such as Educare. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff is carried out regularly, at minimum annually.
- This e-Safety Policy and its updates are presented to and discussed by staff in staff meetings/INSET days.
- A record of concern must be completed by staff as soon as possible if any incident relating to e-Safety occurs and be provided directly to the school's DSL.

### Regarding pupils:

- All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. These behaviours are summarised in the Acceptable Use Policy which must be signed and returned before use of technologies in school. When children use school computers, staff should make sure children are fully aware of the agreement they are making to follow the school's IT guidelines.
- Teaching staff are encouraged to incorporate e-Safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the school community.
- **The e-Safety Co-ordinator** will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- The e-Safety Co-ordinator will provide advice/guidance/training to individuals as required.
- Note: Online Safety BOOST includes an array of presentation resources (<https://boost.swgfl.org.uk/>)

### b. Pupils: e-Safety in the curriculum

The education of pupils in e-Safety is an essential part of the school's e-Safety provision. Children and young people need the help and support of the school to recognise and avoid e-Safety risks and build their resilience. We believe it is essential for e-Safety guidance to be given to pupils on a regular and meaningful basis. We continually look for new opportunities to promote e-Safety and regularly monitor and assess our pupils' understanding of it.

e-Safety should be a focus in all areas of the curriculum and staff should reinforce e-Safety messages across the curriculum. The e-Safety curriculum should be broad, and will be provided in the following ways:



- A planned online safety curriculum should be provided as part of ICT/PSHRE or other lessons and should be regularly revisited
- Key online safety messages should be regularly 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 aware of the impact of cyber-bullying and know how to seek help if these issues affect them (see also the school's Anti-bullying Policy).
- Gidea Park Preparatory School and Nursery will 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 are 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.

By the **end of their time with Gidea Park Preparatory School**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

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

The DfE's statutory guidance 'Keeping Children Safe in Education' obliges schools to "*ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school IT system*", however, schools will need to "*be careful that over blocking does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding*".

Gidea Park Preparatory School and Nursery has a managed ICT service provider, Rika Technologies, who are responsible for the management of the school's technical systems and ensure that the school meets recommended technical requirements for:

- Network security and safety
- Servers, wireless systems and cabling security and safety
- Software licence management and logs
- Secure internet filtering for all users.
- Monitoring and recording inappropriate usage in school
- Reporting and management process for any actual/potential technical incident/security breach

Gidea Park Preparatory School and Nursery systems are remotely managed and monitored on a continuous basis by the IT Manager.

Internet access is filtered for all users through Smoothwall, which is the UK market leader within education, supporting one in three schools to keep pupils safe online.

Differentiated internet access is available for staff and customised filtering changes are managed by the School. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists.

## **9 Password security**

- See Acceptable Use Policy

## **10. Acceptable Use of the Internet in School**

- See Acceptable Use Policy

## **11. Acceptable Use of School Devices**

### **11.2 Pupils**

School mobile devices available for pupil use (including laptops, tablets, etc.) classrooms. Access is available via individual Form Teachers and any use by pupils must be in line with the acceptable use agreement, as set out in appendix 2 of the Acceptable Use Policy.

If pupils bring in their own mobile devices, they must be handed in to Reception at the start of the day and collected as they leave school. These requirements apply to phones and all devices that communicate over the internet, including smartwatches and other wearable technology.

The school recognises that mobile devices are sometimes used by pupils for medical purposes or as an adjustment to assist pupils who have disabilities or special educational needs. Where a pupil needs to use a mobile device for such purposes, the pupil's parents or carers should arrange a meeting the Head to agree how the school can appropriately

support such use. The Head will then inform the pupil's teachers and other relevant members of staff about how the pupil will use the device at school.

## **12 Safe use of digital and video images**

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet.

However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place.

Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees.

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

### **Parents should ensure that:**

- Digital images of their children taken at school events are for their own personal use only
- They respect everyone's privacy and in some cases protection, these images should not be published on blogs or social networking sites (etc.) without the permission of the people identifiable in them (or the permission of their parents), nor should parents comment on any activities involving other pupils in the digital/video images.

**Notes: 1. See school Photography Policy. 2. See Appendix 1 on the use of Tapestry for EYFS.**

## **13 Remote Learning**

All pupils should be aware of the specific 'Acceptable Use for Home Learning' statement which reminds pupils and parents alike of key protocols for safe and polite use of the Internet, see Acceptable Use Policy.

When providing remote learning, teaching staff should:

- Adhere to the AUP principles ensuring that all communication with parent/pupils should be via school channels only
- Abide by the staff code of conduct
- Apply normal safeguarding procedures and protocols; DSL or DDSL always available during school hours

- Consider the wellbeing and mental health of each pupil – how they feel; their home and immediate family circumstances which may impact on their ability to participate in remote learning.

In addition:

- parents should remember that teachers may only be contacted during the normal school day.

Access to additional education software provided via remote learning (e.g. IXL) is used to support the remote curriculum and provide relevant content and exercises for pupils. Each has been selected based on fit with the curriculum; ease of use; reputation and track record for security and privacy.

## 14 Cyber-bullying

### 14.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

**Note: See also the school behaviour policy.**

### 14.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form teachers will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes PSHRE education, and other subjects where appropriate.

All staff, directors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external agencies if it is deemed necessary to do so.

### 14.3 Examining electronic devices (including ipads issued to children)

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on [screening, searching and confiscation](#).

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

**Note: Please also refer to our Safeguarding and Anti-Bullying Policies.**

## 15. Responding to issues of misuse

**Where a pupil** misuses the school's ICT systems or internet, we will follow the procedures set out in our Behaviour Policy or Anti-Bullying Policy. The action taken and sanctions imposed will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

**Where a staff member** misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the relevant School procedures and policies which include:

- Staff disciplinary procedures
- Staff code of conduct

The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

## 16. Responding to Incidents

The first response should be to establish the nature of the incident and level of concern.

The Online Safety Incident Flowchart (page 16) provides helpful guidance for use in managing e-Safety incidents. It encourages a safe and secure approach to the leadership of the incident and

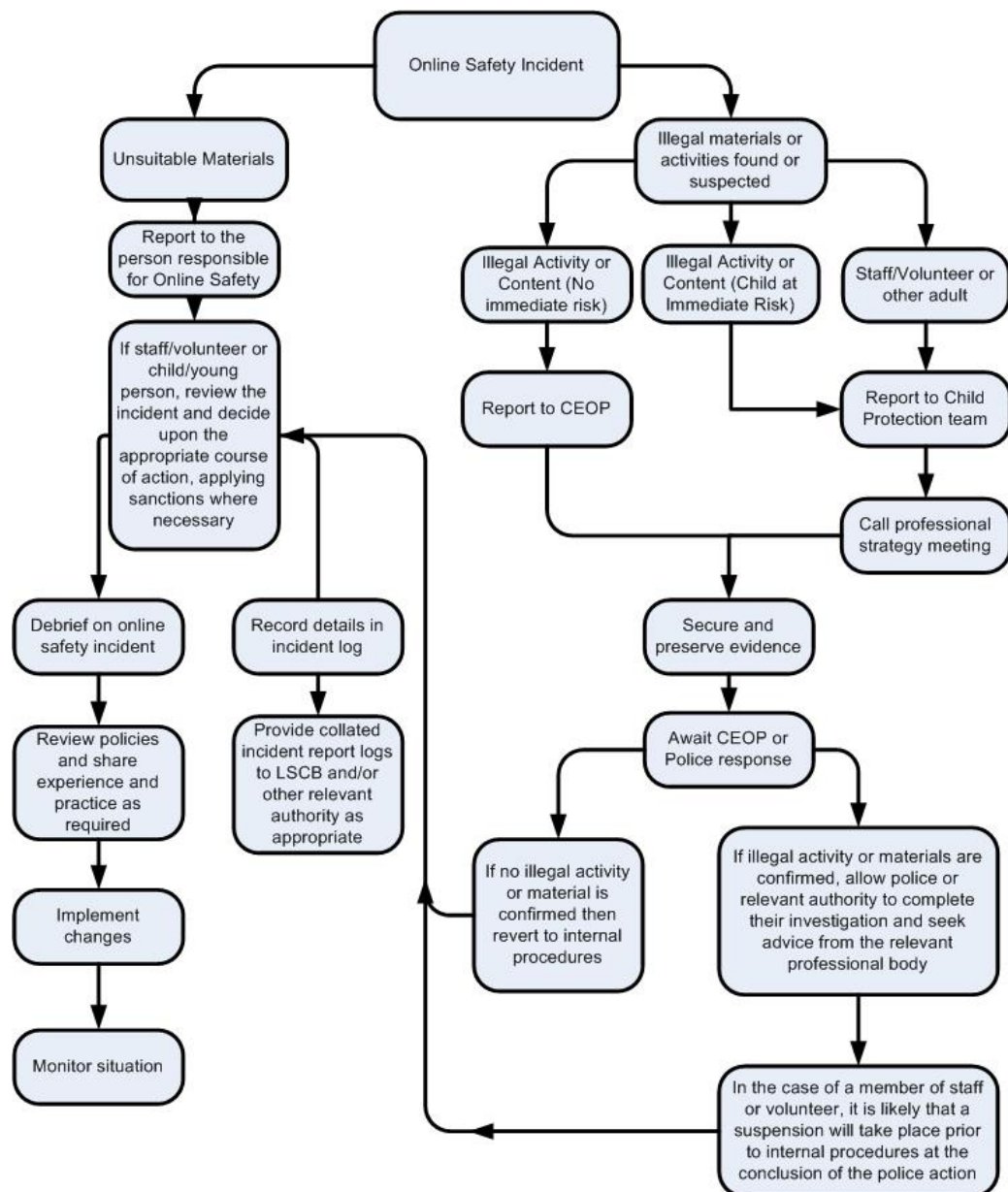
underlines the importance of establishing as soon as possible whether the incident relates to **unsuitable** materials or **illegal** materials/ actions.

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

- The Head/DSL should be informed. If they are not available, a DDSL should be informed. They will oversee the initial investigation, involving only those parties relevant to the incident and with appropriate expertise. This may include the IT Manager, J Woods.
- An initial investigation should be conducted using a designated computer removed from general use (to ensure no access by pupils or unauthorised staff), that could also, if necessary, be taken off site by the police. The same computer will be used for the duration of the procedure.
- A record should be made of all sites, URL and content visited during the investigation and screenshots should be recorded if appropriate in the incident log, shown in appendix 2.
- **If illegal content or a safeguarding concern** is confirmed, this should immediately be reported to Havering MASH (and the Police if appropriate). The Havering Flowchart for raising a safeguarding concern will then be followed (Safeguarding Policy Page 11 and Appendix 3)
- **If unsuitable materials or inappropriate use** are established this will be dealt with as outlined in point 14.

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

**Notes: See Child Protection and Safeguarding Policy for further details.**



## 17. Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and its update, the General Data Protection Regulation May 2018, which states that personal data must be:

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

**The school must ensure that:**

- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- It holds the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary
- Every effort should be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay
- All personal data should be fairly obtained in accordance with the “Privacy Notice” and lawfully processed in accordance with the “Conditions for Processing”
- It takes particular care with sensitive personal data
- It shares data only with those with legitimate rights to see said data

**Staff must ensure that they:**

- Take care at all times to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.
- Abide by password security protocols e.g. do not write passwords down; do not share passwords; use a strong password.

**Notes: See Data Protection and Privacy Notices for full details.**

## 18. Complaints

As with all issues of safety, if a member of staff, a pupil or a parent/carer has a complaint or concern relating to e-Safety, prompt action will be taken to deal with it.

Concerns should be addressed to the e-Safety Co-ordinator in the first instance, who will liaise with the Head and undertake an investigation where appropriate.

Incidents or concerns around e-Safety will be recorded using a Record of Concern Form and the investigation will be recorded in the Incident Log.

Where a concern or complaint escalates and becomes a safeguarding concern then the Designated Safeguarding Lead, Mrs Whiskerd, will take the lead and will manage the incident in accordance with the school's Safeguarding Policy.

All other e-Safety complaints will be managed according to our normal complaints procedures.

**Please see the Complaints Policy for further information.**



## **APPENDIX 1**

### **Early Years Foundation Stage: Tapestry Software**

#### **Abbreviated Privacy and Security Policies**

1. **Who is Tapestry?** Tapestry is the name of a product that was conceived, developed and is owned by The Foundation Stage Forum Ltd. (The FSF), an early year's organisation that has provided resources and support for the early years (EYFS) workforce since February 2003.
2. **Who owns the data?** Gidea Park Preparatory School and Nursery owns the data and is the Data Controller. Tapestry is the Data Processor and cannot do anything with our data without our express permission.
3. **Registration with the Information Commissioner's Office (ICO):** Tapestry is registered with the ICO under number: Z1783069 and must conform to the data protection principles as laid out in Schedule 1 of the Data Protection Act.
4. **Access to data:** Is restricted to those who are specifically authorised to view and add/delete/change data. Access is restricted and designed to minimise access to data and photos. This is controlled through the use of passwords.
5. **Technical data security:** The Tapestry web service and data are hosted in a cloud hosting environment operated by AWS in the EU (primarily the Republic of Ireland). AWS is the largest cloud hosting provider in the world and provides a secure platform for some of the world's largest on-line service providers. The ensure that:
  - The servers are physically secure
  - Software is secure: regular automated tests, internal security review, virus checks.
  - Connections are encrypted.
  - Tapestry uses Enhanced Validation Certification (EVC) to offer visible assurance that the service is provided by a validated organisation.
  - The network is partitioned to provide minimum access between servers and the internet; and to Gidea Park's data is held on separate database from any other school to ensure our data is not compromised.
  - Logs are held of all activity on the Tapestry system
  - Accredited, independent firms conduct Penetration Testing – most recently in 2016
  - Capacity, redundancy and backups are all stored in at least 2 separate physical locations.

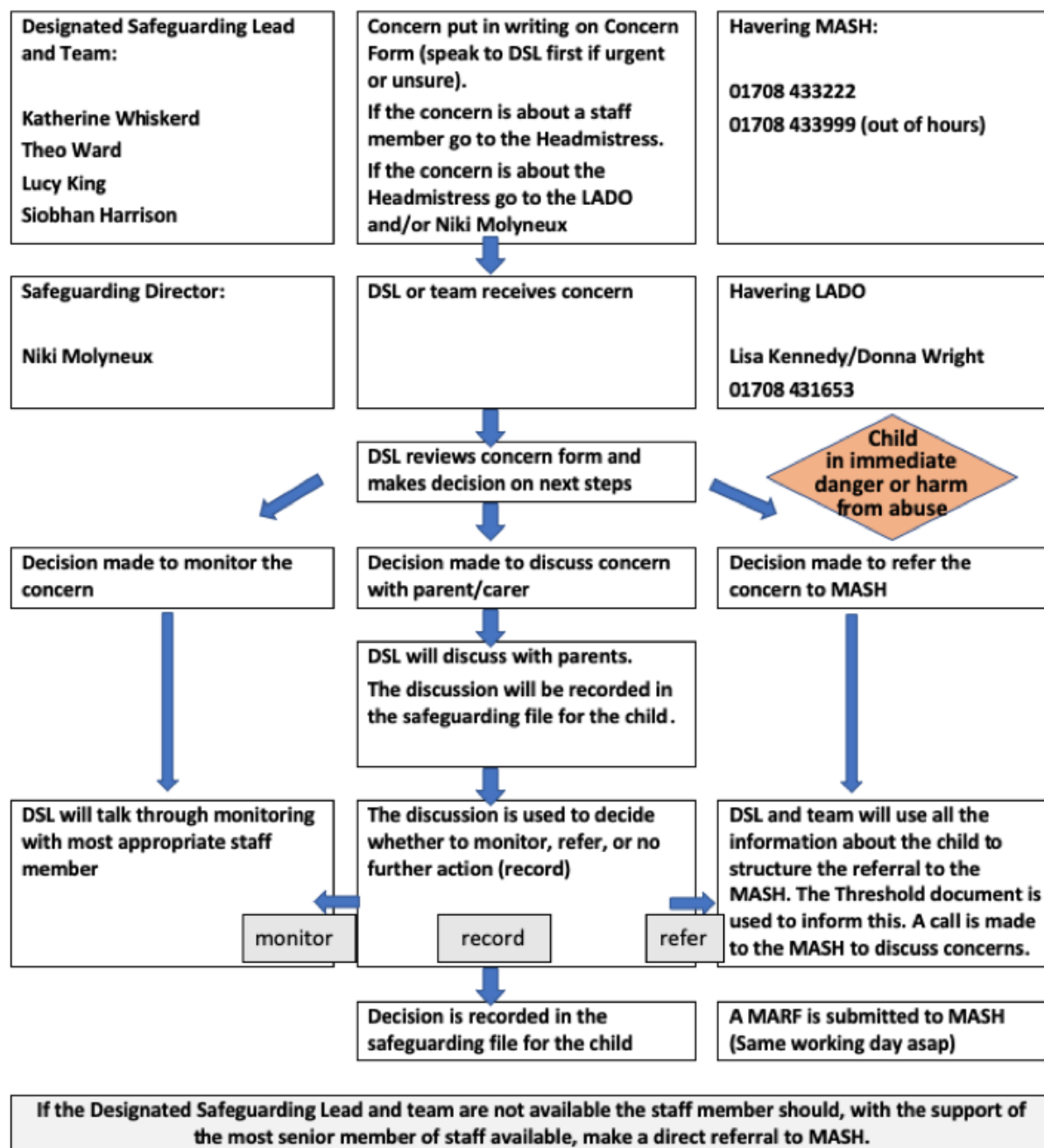
**Note:** Tapestry's full Privacy and Security Policies are available on the School's central server for reference.

## **APPENDIX 2**

ONLINE SAFETY INCIDENT LOG				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident

## APPENDIX 3

### HAVERING FLOWCHART FOR RAISING CONCERNS



## **APPENDIX 4**

### **Links to other organisations or documents**

Safer Internet Centre

<https://www.getsafeonline.org/>

South West Grid for Learning

Childnet

[Child Exploitation and Online Protection Centre](#) - a National Crime Agency command dealing with criminal / safeguarding concerns and reporting

[NSPCC Child abuse and neglect guidance](#)

Professionals Online Safety Helpline

Internet Watch Foundation

CEOP

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

[ThinkUKnow](#)

### **Others**

INSAFE - <http://www.saferinternet.org/ww/en/pub/insafe/index.htm>

UK Council for Child Internet Safety (UKCCIS) [www.education.gov.uk/ukccis](http://www.education.gov.uk/ukccis)

Netsmartz <http://www.netsmartz.org/index.aspx>

### **Support for Schools**

Specialist help and support [SWGfL BOOST](#)

### **Cyberbullying**

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

Scottish Government - [Better relationships, better learning, better behaviour](#)

DCSF - Cyberbullying guidance

DfE – Preventing & Tackling Bullying – Advice to school leaders, staff and Governing Bodies

Anti-Bullying Network - <http://www.antibullying.net/cyberbullying1.htm>

Cyberbullying.org - <http://www.cyberbullying.org/>

### **Social Networking**

Digizen – [Social Networking](#)

[SWGfL - Facebook - Managing risk for staff and volunteers working with children and young people](#)

[Connectsafely Parents Guide to Facebook](#)

[Facebook Guide for Educators](#)

### **Curriculum**

[SWGfL Digital Literacy & Citizenship curriculum](#)

Glow - <http://www.educationscotland.gov.uk/usingglowandict/>

Alberta, Canada - [digital citizenship policy development guide.pdf](#)

Teach Today – [www.teachtoday.eu/](http://www.teachtoday.eu/)

Insafe - [Education Resources](#)

Somerset - [e-Sense materials for schools](#)

## **APPENDIX 5**

### **Guidance**

It is not a specific requirement of the Education (Independent School Standards) Regulations 2014 for independent schools to have an e-Safety policy. However, with the increasing availability of devices which give unrestricted access to the internet for children, schools should consider online safety in parallel with safeguarding and anti-bullying procedures.

The ISI Handbook September 2020 states (at paragraphs 303 - 304):

303. It is not a requirement to have a separate cyber-bullying policy, but with increasing availability to children of electronic devices that give unrestricted access to the internet, schools should consider online safety as part of both safeguarding and anti-bullying arrangements. Active management of hardware, software and connectivity and the vigilance of teachers and parents have a part to play in the safeguarding and protection of pupils.
304. Pupils will often have access to technologies that have both positive and negative potential. Consideration should be given to the acceptable use of technology within the school setting and beyond, with a policy that is clear, understood and respected by staff, pupils and the wider school community. Whilst each school's perspective and practice will vary, the policy should ensure the school's expectations and safeguarding obligations are communicated and effective. A policy should include guidance on:
- clearly defined roles and responsibilities for online safety as part of the school's wider safeguarding strategy and how this links with other safeguarding policy;
  - clear guidance on the use of technology in the classroom and beyond for all users, including staff, pupils and visitors that references permissions/restrictions and agreed sanctions;
  - mention of the school's technical provision/infrastructure and safeguards in place to filter and monitor inappropriate content and alert the school to safeguarding issues; (schools are not required to give away detail in policies which would compromise safeguards);
  - how the school builds resilience in its pupils to protect themselves and their peers through education and information;
  - staff safeguarding professional development that includes online safety;
  - reporting mechanisms available for all users to report issues and concerns to the school and how they are managed and/or escalated;
  - how the school informs, communicates with and educates parents/carers in online safety;
  - the management of personal data in line with statutory requirements.

Keeping Children Safe in Education statutory guidance for schools and colleges (January 2021) endorses a '*whole school approach to online safety*' and explains that this '*will include a clear policy on the use of mobile technology in the school*'.

The DfE's Boarding Schools National Minimum Standards (in force from 1 April 2015) requires schools to have and implement a policy that includes measures to combat cyber bullying.

The DfE's Statutory framework for the Early Years Foundation Stage (**EYFS**) (September 2014) refers to the need, in a safeguarding context, for school policies to cover the use of mobile phones and cameras.

The DfE's guidance on the 'prevent duty' (the duty in the Counter-Terrorism and Security Act 2015 on specified authorities, in the exercise of their functions, to have due regard to the need to

prevent people from being drawn into terrorism), refers to the need for schools to ensure children are safe from terrorist and extremist material when they access the internet in schools and to ensure that schools put in place suitable filtering systems.

The South West Grid for Learning strongly recommends "*that each school should have a named member of staff with a day to day responsibility for e-Safety, some schools may choose to combine this with the Child Protection / Safeguarding Officer role. Schools may choose to appoint a person with a child welfare background, preferably with good knowledge and understanding of the new technologies, rather than a technical member of staff - but this will be the choice of the school.*"

### **Privacy implications of mobile devices**

Any device that accesses a communications network potentially gives rise to e-Safety issues. The most obvious examples of such devices are computers and phones, but an increasing variety of other devices also access such networks. For example, many wristwatches and items of jewellery are capable of recording and transmitting data about the wearer and his or her environment. Some of these devices are marketed at parents, to enable them to remotely monitor their children's whereabouts and social interactions. Such devices may offer safety benefits, but they may also impinge on the privacy of the wearer and those in his or her immediate environment.

## Appendix 6 – e-Safety @ Gidea Park

**Pre-Prep** - Use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

**Prep** - use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content

### Features associated with resilience

- Planning tendency (propensity to plan).
- A style of self-reflection as to what worked and what didn't work.
- A sense of agency or determination to deal with challenge.
- Self-confidence in being able to deal with challenges successfully.

### Understand

An individual understands when they are at risk online and can make informed decisions about the digital space they are in

### Know

An individual knows what to do to seek help from a range of appropriate sources

# DIGITAL RESILIENCE

### Learn

An individual learns from their experiences and is able to adapt their future choices, where possible

### Recover

An individual can recover when things go wrong online by receiving the appropriate level of support to aid recovery

## Other good resources

<a href="#">Childnet</a>	<a href="#">Cyberbullying info</a>
<a href="#">Google Internet legends game</a>	<a href="#">Childline</a>
<a href="#">Google Scheme of work</a>	<a href="#">E-safety materials</a>
<a href="#">e-safety policy</a>	<a href="#">Acceptable Usage Policy</a> (AUP)

Year Group	E-Safety Objectives	Resource ideas	Lesson ideas
<b>EYFS</b>	<b>Learning Objectives:</b>	<b>Teaching Points:</b>	<b>Possible Resources:</b>
Online Exploration	<ul style="list-style-type: none"> <li>• Be aware that they can use the internet to play and learn, supported by a trusted adult/teacher.</li> <li>• Begin to understand the difference between real and online experiences.</li> <li>• Recognise the impact of good choices and consequences of wrong ones.</li> <li>• Know that information can be retrieved from computers and can tell an adult if what they see makes them feel worried.</li> </ul>	<ul style="list-style-type: none"> <li>• Children need help from their teacher or trusted adult before they go online.</li> <li>• Children explore onscreen activities that mimic real life.</li> <li>• Children talk about the differences between real and online experiences.</li> </ul>	<p>Access online resources, e.g.;</p> <ul style="list-style-type: none"> <li>• <a href="#">ICT Games</a></li> <li>• <a href="#">Cbeebies games</a></li> <li>• <a href="#">Fun with Spot</a></li> </ul> <p>Get the children to scan QR codes to the websites you want them to visit</p> <ul style="list-style-type: none"> <li>• Jessie and Friends <a href="#">Episode 1 - Watching Videos (4-5 years)</a></li> <li>• <a href="#">Book</a> (also saved on the Network)</li> </ul>
Online Communication & E-Awareness	<ul style="list-style-type: none"> <li>• Children know that they can use the internet to communicate with family and friends.</li> <li>• For children to understand the importance of politeness and courtesy on and off the internet.</li> <li>• Children will be aware of how to keep safe and what to do if they are concerned.</li> </ul>	<ul style="list-style-type: none"> <li>• Children begin to understand that they can share information online, e.g. via Tapestry / Purple Mash</li> <li>• Children begin to understand that there is a right and wrong way to communicate and this may be different depending on who you are communicating with.</li> </ul>	<ul style="list-style-type: none"> <li>• <a href="#">Sebastian Swan</a> – visit Sebastian’s blog and contact Sebastian Swan</li> <li>• <a href="#">Smartie The Penguin</a> story from KidSMART <ul style="list-style-type: none"> <li>• Time to Chat to accompany the Smartie e-book.</li> </ul> </li> </ul>



Form I	Learning Objectives:	Teaching Points:	Possible Resources:
Online Research	<ul style="list-style-type: none"> <li>• Children understand that they can find a range of information on the internet.</li> <li>• Children are able to navigate age-appropriate websites.</li> <li>• Children know what to do if they find something inappropriate online.</li> <li>• Discuss common uses of IT beyond school</li> <li>• Children recognise the Internet as an exciting place to be but understand the need for a balance in how they spend their time and make good choices about age-appropriate activities.</li> </ul>	<ul style="list-style-type: none"> <li>• Use simple navigation skills to open a teacher selected website from a bookmarked link, QR code or shortcut.</li> <li>• Make choices by clicking on buttons in a webpage and navigate between pages by using the forward and back arrows.</li> <li>• Start to evaluate web sites by giving opinions about preferred or most useful sites.</li> <li>• Know how to return to the home page of a teacher directed website.</li> <li>• Know how to minimise a screen if they see something inappropriate on a website and then tell a trusted adult.</li> </ul>	<ul style="list-style-type: none"> <li>• Variety of websites, suitable for online research and exploration, e.g.</li> <li>• <a href="#">ICT Games</a></li> <li>• <a href="#">Cbeebies games</a></li> <li>• <a href="#">DK find out</a></li> </ul>

Communication & Collaboration	<ul style="list-style-type: none"> <li>Children know that there are a variety of online tools that can be used to communicate with other people.</li> </ul>	<ul style="list-style-type: none"> <li>Know that email is a method of sending and receiving messages through the Internet.</li> <li>Participate in the sending of class emails.</li> <li>Understand the need to keep passwords private.</li> </ul>	<ul style="list-style-type: none"> <li>CEOP Thinkuknow resources, based on Hector's World <ul style="list-style-type: none"> <li><a href="http://www.thinkuknow.co.uk/5_7/">www.thinkuknow.co.uk/5_7/</a> (lessons 1 – 5)</li> </ul> </li> <li>School email or messaging system through Showbie</li> <li>Role-play how to talk kindly and politely to friends online and in the real world, and how to comment kindly on people's work.</li> </ul>
Awareness	<ul style="list-style-type: none"> <li>Children begin to identify characteristics of people who are worthy of their trust.</li> <li>For children to know what action to take if they feel they may be in danger.</li> <li>Understand the uses of ICT inside and outside of school and to use it responsibly.</li> <li>Children begin to understand what personal information is and who you can share it with, including the need to keep passwords private.</li> </ul>	<ul style="list-style-type: none"> <li>Know that some information (full name, address, birthday etc...) is special as it applies to them.</li> <li>Children know that personal information is as valuable online as offline and that it should not be shared without a parent, carer or teacher's permission.</li> <li>Children discuss, understand and abide by the school's e-Safety or Internet Acceptable usage policy.</li> <li>To understand the importance of talking to a trusted adult about their online experiences.</li> </ul>	<ul style="list-style-type: none"> <li><a href="#">Log in securely on Showbie/Bugclub</a></li> <li>CEOP Thinkuknow resources, based on <a href="#">Hector's World</a></li> <li><a href="#">Smartie The Penguin</a> story from KidSMART</li> <li><a href="#">Digiduck's Big Decision – saved on the system</a></li> <li>Jessie and Friends <a href="#">Episode 2</a> – Sharing Pictures (5-6 years)</li> <li><a href="#">Book</a> – saved on system also</li> </ul>
<b>Form 2</b>	<b>Learning Objectives:</b>	<b>Teaching Points:</b>	<b>Possible Resources:</b>
Online Research	<ul style="list-style-type: none"> <li>Children use the internet purposefully to answer specific questions.</li> <li>Children know that not everything they encounter on the internet is true.</li> <li>Children know who to tell when they see something that makes them uncomfortable and make sure an adult knows what they are doing.</li> </ul>	<ul style="list-style-type: none"> <li>Children explore a range of age-appropriate digital resources.</li> <li>Children to know that not everything they find online is accurate.</li> <li>Know that some websites contain advertisements (often embedded) and learn how to ignore them.</li> <li>Children to know what to do if they find something inappropriate online.</li> <li>Children discuss, understand and abide by the school's e-Safety/AUP.</li> </ul>	<ul style="list-style-type: none"> <li>Agree sensible e-safety rules for the classroom.</li> <li><i>Download and use Hector's World Safety Button (used to cover the screen if children find something they think maybe unsafe).</i></li> <li>Websites to aid research, e.g.; Barnaby website to find out about his trips and how he travels.</li> <li>Use a selection of websites and consider who can see the information online. (These are best linked to topics being taught in class)</li> </ul>


Communication & Collaboration	<ul style="list-style-type: none"> <li>Children know the difference between communicating via email and online in a discussion forum.</li> <li>Children are aware of the different forms of online communication (email, forums, instant messaging and social networking sites) and find out about their associated risks.</li> </ul>	<ul style="list-style-type: none"> <li>Children are able to send suitable and purposeful online messages, developing awareness of appropriate language to use.</li> <li>Children know that passwords help to keep information safe and secure and that they should not be shared Children contribute to a class discussion forum.</li> </ul>	<a href="#">Digiduck's Famous Friend</a> (also saved on the system)  Discussion forums/ blog or messaging system on Showbie
E-Awareness	<ul style="list-style-type: none"> <li>Develop awareness of relevant e-Safety issues and understand that personal information is unique to them.</li> <li>Identify characteristics of people who are worthy of their trust.</li> <li>For learners to be aware of, and able to use, the rules for keeping safe on the internet.</li> <li>For learners to understand the uses of ICT inside and outside of school and to use it responsibly.</li> <li>Children recognise the Internet as an exciting place to be but understand the need for a balance in how they spend their time and make good choices about age-appropriate activities</li> </ul>	<ul style="list-style-type: none"> <li>Children are aware that not everyone they meet online is automatically trustworthy.</li> <li>Children understand that personal information is unique to them and should not be shared without a teacher or parent's permission.</li> <li>Children identify characteristics of people who are worthy of their trust.</li> </ul>	<ul style="list-style-type: none"> <li>Jessie and Friends <a href="#">Episode 3</a> – Playing Games (6-7 years)</li> <li><a href="#">Book</a> – saved on system also</li> </ul>
<b>Form 3</b>	<b>Learning Objectives:</b>	<b>Teaching Points:</b>	<b>Possible Resources:</b>
Online Research	<ul style="list-style-type: none"> <li>Children develop strategies for staying safe when searching for content whilst using the Internet.</li> <li>Children to use the Internet to undertake independent and appropriate research and attempt to distinguish between fact and fiction.</li> </ul>	<ul style="list-style-type: none"> <li>Use child-friendly search engines independently to find information through key words.</li> <li>Identify ways of working out whether information online is reliable. (Tree octopus)</li> <li>Reinforce the rule about keeping adults informed about Internet activity and telling if you see something you don't like or if you feel you're being bullied.</li> </ul>	Discuss and agree classroom rules / expectations about safe use of the Internet. <a href="#">Fake News - tree octopus</a>  Inaccurate information online; Captain Kara and Winston's SMART Adventure (KnowITall), chapter 2, <a href="#">"What is Reliable?"</a>

Communication & Collaboration	<ul style="list-style-type: none"> <li>• Children begin to use a range of online communication tools, such as forums, email and polls in order to formulate, develop and exchange ideas.</li> </ul>	<ul style="list-style-type: none"> <li>• Use a range of online communication tools, such as email, forums and polls.</li> <li>• Know how to deal with unpleasant forms of electronic communication (save the message and speak to a trusted adult).</li> <li>• Be able to discern when an email should or should not be opened.</li> </ul>	<p>Unsolicited emails and attachments; Captain Kara and Winston's SMART Adventure (KnowITall), chapter 1, <a href="#">"What should you keep Accept?"</a></p> <p>Captain Kara and Winston's SMART Adventure (KnowITall), Chapter 4, <a href="#">"Who should I tell?"</a></p>
E-Awareness	<ul style="list-style-type: none"> <li>• Children develop awareness of online protocols, in order to stay safe on the web.</li> <li>• Children develop understanding of the SMART rules in relation to safe use of the Internet.</li> <li>• Children understand that any personal information they put online can be seen and used by others</li> </ul>	<ul style="list-style-type: none"> <li>• Develop awareness of relevant e-Safety issues, such as cyber bullying.</li> <li>• Children understand and abide by the school's AUP and know that it contains rules that exist in order to keep children safe online.</li> <li>• Understand what personal information should be kept private.</li> <li>• Know that passwords keep information secure and that they should be kept private.</li> <li>• Demonstrate ways of protecting their online reputation.</li> </ul>	<p>Personal information; Inaccurate information online; Captain Kara and Winston's SMART Adventure (KnowITall), chapter 3, <a href="#">"What should you keep Safe?"</a></p> <p>Captain Kara and Winston's SMART Adventure (KnowITall), chapter 5, <a href="#">"Be careful when meeting up?"</a></p> <p>Google E-safety – saved on system. Be internet sharp, Be internet aware</p>

Form 4	Learning Objectives:	Teaching Points:	Possible Resources:
Online Research	<ul style="list-style-type: none"> <li>• Children safely use the Internet for research and follow lines of enquiry.</li> <li>• Children understand the function of a search engine and the importance of using correct search criteria.</li> <li>• Children use the internet as a resource to support their work, and begin to understand plagiarism.</li> </ul>	<ul style="list-style-type: none"> <li>• Use internet search engines to gather resources for their own research work.</li> <li>• Be aware of different search engines and discuss their various features (e.g. Google image &amp; video search).</li> <li>• Understand the importance of framing questions into search criteria when conducting web searches.</li> </ul>	<p>Spoof websites:  <a href="http://www.allaboutexplorers.com">www.allaboutexplorers.com</a>  <a href="#">Fake News - Dog Island</a>            ThinkUKnow game, <a href="#">"Responsible use of the internet"</a> (<a href="#">teacher page</a>)</p> <p><b>Create your own SMART rules poster</b>  <a href="#">SMART rules</a></p>

	<ul style="list-style-type: none"> <li>Children know that not everything they find on the Internet is true and know what to do if they find something they are uncomfortable with <b>including cyberbullying</b>.</li> </ul>	<ul style="list-style-type: none"> <li>Be aware that not everything they find online is accurate and that information needs to be checked and evaluated.</li> </ul>	
Communication & Collaboration	<ul style="list-style-type: none"> <li>Children use a range of communication tools to collaborate and exchange information with others, e.g. email, blog, forums.</li> <li>They recognise that they can use online tools to collaborate and communicate with others and the importance of doing this responsibly, choosing age-appropriate websites.</li> <li>Know what to do if they find something they are uncomfortable with <b>including cyberbullying</b></li> </ul>	<ul style="list-style-type: none"> <li>Children use online communication tools to exchange and develop their ideas in a range of curriculum opportunities.</li> <li>Use sensitive and appropriate language when using online communication tools.</li> <li>Use email as a form of communication, use the "To" box and add a subject heading.</li> <li>Add an attachment to an email.</li> <li>Develop understanding of when it is unsafe to open an email or an email attachment.</li> </ul>	ThinkUKnow <a href="https://gridclub.com/activities/cybercafe">Bandrunner videos</a> <a href="https://gridclub.com/activities/cybercafe">https://gridclub.com/activities/cybercafe</a>
E-Awareness	<ul style="list-style-type: none"> <li>Understand and abide by the schools acceptable use policy.</li> <li>Children are aware of the need to develop a set of online protocols in order to stay safe online.</li> <li>Children develop awareness of relevant esafety issues.</li> <li>Recognise the need to choose age-appropriate games to play and when to limit use.</li> </ul>	<ul style="list-style-type: none"> <li>Children understand and abide by the school Internet Acceptable Usage Policy (AUP) and aware of the implications of not following the rules.</li> <li>Children understand that a password can keep information secure and the need to keep it a secret.</li> </ul>	<a href="http://www.thinkuknow.co.uk/professionals/resources/online-toolkits-online-version/">www.thinkuknow.co.uk/professionals/resources/online-toolkits-online-version/</a>  <a href="https://www.esafety.gov.au/educators/classroom-resources/be-secure">https://www.esafety.gov.au/educators/classroom-resources/be-secure</a>  Google E-safety – saved on system. Be Internet Secure & Be Internet Kind

Form 5	Learning Objectives:		Teaching Points:	Possible Resources:
Online Research	<ul style="list-style-type: none"><li>• Children develop their online set of protocols in order to keep safe online.</li><li>• Children recognise inaccuracy and bias on the web and evaluate websites for their validity.</li></ul>	<ul style="list-style-type: none"><li>• When using the Internet to research their work, children recognise the need to ask appropriate questions to find appropriate answers.</li><li>• Children know that good online research involves interpreting information, rather than copying.</li></ul>	<a href="#">Fake News - Petrol Direct</a>  For copyright free pictures and music; <a href="#">NEN Gallery</a>	

	<ul style="list-style-type: none"> <li>Children understand appropriate and inappropriate use of the Internet including excessive use.</li> <li>Children recognise the risks and rewards of using Internet communication tools and understand how to protect themselves and the devices they use.</li> </ul>	<ul style="list-style-type: none"> <li>Children are able to carry out more refined web searches by using key words.</li> <li>Children evaluate search results and refine as necessary for the best results.</li> <li>Know that information found on websites may be inaccurate or biased and to check the validity of a website.</li> <li>Develop strategies to ignore or cancel unsolicited advertising (pop-ups, banners, videos or audio).</li> <li>Children use websites where resources can be downloaded without infringing copyright.</li> </ul>	 <p><b>ZIP IT</b> Keep your personal stuff private and think about what you say and do online.</p> <p><b>BLOCK IT</b> Block people who send nasty messages and don't open unknown links and attachments.</p> <p><b>FLAG IT</b> Flag up with someone you trust if anything upsets you or if someone asks to meet you offline.</p>
Communication & Collaboration	<ul style="list-style-type: none"> <li>Children use online tools to exchange information and collaborate with others within and beyond their school and begin to evaluate their effectiveness.</li> <li>Children understand the need to respect the rights of other users, and understand their own responsibility for information that is shared and how it may impact on others.</li> </ul>	<ul style="list-style-type: none"> <li>Be aware of the different forms of technology that can be used to access the Internet and communicate with others.</li> <li>Use sensitive and appropriate language when using online communication tools.</li> </ul>	<ul style="list-style-type: none"> <li>Cybersmart Challenge – <a href="#">teacher resources</a></li> <li><a href="#">Cybersmart Forever</a> (35 to 45 mins) focusing on the risks of sharing images online</li> <li><a href="#">Cybersmart Detectives</a> (30 to 45 mins) focusing on privacy, personal information and inappropriate or unwanted contact</li> <li><a href="#">Cybersmart Hero</a> (35 to 45 mins) focusing on cyberbullying and the role of the bystander</li> </ul>
E-Awareness	<ul style="list-style-type: none"> <li>Children understand the potential risks of providing personal information in an increasing range of online technologies both within and outside school.</li> <li>Children understand the need to keep personal information and passwords private, and know how to choose a secure password.</li> </ul>	<ul style="list-style-type: none"> <li>Children recognise their own right to be protected from the inappropriate use of technology by others and the need to respect the rights of other users.</li> </ul>	<p>Internet Safety Games from Thinkuknow</p> <p><b>Horrible Histories videos:</b></p> <p>Guy Fawkes – <a href="#">Internet Privacy Settings</a></p> <p>Prudish Victorian – <a href="#">Don't Lie About Your Age Online</a></p> <p>Saxon Monk – <a href="#">Internet Videos are Forever</a></p> <p>Lady Jane Grey – <a href="#">Beware What You Download</a></p> <p>Google E-safety – saved on system. Be Internet Sharp Think Before You Share AND Check it's For Real</p>

Form 6	Learning Objectives:	Teaching Points:	Possible Resources:
Online Research	<ul style="list-style-type: none"> <li>Children confidently and competently use the Internet as a tool for research and critically <del>evaluate websites for their use.</del></li> </ul>	<ul style="list-style-type: none"> <li>Use a range of sources to check the validity of a website.</li> </ul>	Website searching linked to in class topics

	<ul style="list-style-type: none"> <li>Children know that information they find on the Internet is often inaccurate or biased and develop strategies for identifying the origin of a website.</li> <li>Children are aware of copyright issues and know that not all resources they find on the Internet are legal to use or copy (even if sources are acknowledged).</li> </ul>	<ul style="list-style-type: none"> <li>Recognise that different viewpoints can be found on the web.</li> <li>Critically evaluate the information they use, and understand some of the potential dangers of not doing so.</li> <li>Be aware of the issues of plagiarism, copyright and data protection in relation to their work.</li> <li>Select copyright free images and sounds from sources such as the Audio Networks and NEN image gallery.</li> </ul>	
Communication & Collaboration	<ul style="list-style-type: none"> <li>Select appropriate tools to collaborate and communicate confidently and safely with others within and beyond their school.</li> <li>Understand how to protect themselves from cyberbullying or causing hurt to others, especially when using social networks (including online gaming communities).</li> </ul>	<ul style="list-style-type: none"> <li>Decide which online communication tool is the most appropriate to use for a particular purpose, e.g. email, discussion forums, podcast, or messaging tools in the learning platform.</li> </ul>	<p>Networking – <b>Showbie</b></p> <p>Safe Profiling School email system or communication tools within the learning platform.</p> <p><a href="#">Game on Teachers</a></p> <p><a href="#">Game on pupils</a></p>
E-Awareness	<ul style="list-style-type: none"> <li>Children evaluate their use of technology including the use of email, social networking, online gaming and mobile phones and consider how they present themselves online.</li> <li>Children understand how to use social networking websites appropriately, keeping an adult informed about their online activity.</li> </ul>	<ul style="list-style-type: none"> <li>Be aware of the issues surrounding cyberbullying and understanding the impact on an individual of sending or uploading unkind or inappropriate content.</li> <li>Know that malicious adults use the Internet and attempt to make contact with children and know how to report abuse.</li> </ul>	<p><a href="http://www.thinkuknow.co.uk/teachers/">http://www.thinkuknow.co.uk/teachers/</a></p> <p><b>Horrible Histories videos:</b></p> <p>Guy Fawkes – <a href="#">Internet Privacy Settings</a></p> <p>Prudish Victorian – <a href="#">Don't Lie About Your Age Online</a></p> <p>Saxon Monk – <a href="#">Internet Videos are Forever</a></p> <p>Lady Jane Grey – <a href="#">Beware What You Download</a></p> <p><a href="#">Jigsaw video from CEOP</a></p> <p><a href="#">“Let's fight it together”</a> Cyberbullying section, accompanied by comprehensive teaching resources and video</p> <p>Google E-safety – saved on system. Be Internet Secure - Protect Your Stuff AND Be Internet Kind - Respect Each</p>