



## Kelford School Online Safety Policy

<b>Date Published</b>	<b>June 2016</b>
<b>Version</b>	<b>3</b>
<b>Approved Date</b>	<b>January 2018</b>
<b>Review Cycle</b>	<b>Biennial</b>
<b>Next Review Date</b>	<b>May 2024</b>

An academy within:



“Learning together, to be the best we can be”



# 1. Overview

- 1.1. Kelford School is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment. This policy was created by the Safeguarding Team and approved by Nexus MAT. This policy will be reviewed annually.

# 2. Introduction

- 2.1. In today's society, children, young people and adults interact with technologies such as mobile phones, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger.
- 2.2. E-safety covers issues relating to children and young people as well as adults and their safe use of the Internet, mobile phones and other electronic communications technologies, both in and out of school. It includes education for all members of the school community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children.
- 2.3. As well as being a National Curriculum requirement in the form of Computing, the ability to use Information and Communications Technology (ICT) effectively is an important life-skill for all our pupils. ICT should help all our pupils to develop the skills and capabilities they need to become:
  - **Successful learners** who enjoy learning, make progress and achieve;
  - **Confident individuals** who are able to lead safe, healthy and fulfilling lives; and
  - **Responsible citizens** who make a positive contribution to society.
- 2.4. At Kelford, ICT includes the use of any equipment which helps pupils to communicate, use information and control their environment. This includes the use of computers (including the internet), switches, programmable toys and control kits, assistive technology (specialist key pads, overlay keyboards, touch screens), sensors and probes, electronic musical instruments (including Sound beam), audio and video recorders, telephone and fax machines, digital cameras, scanners and voice activated equipment.
- 2.5. Benefits of using the Internet in education include:
  - access to worldwide educational resources including museums and art galleries;
  - educational and cultural exchanges between pupils worldwide;
  - access to learning wherever and whenever its convenient.



2.6. The school has a legal duty to ensure that it has done all in its power to protect users of the system and to keep sensitive data safe and secure. This Online Safety policy is an honest attempt to cover all the main areas, and sets out how we plan to develop and establish our Online Safety approach and to identify core principles which all members of the school community need to be aware of and understand.

## 2.7. Responsibilities

2.7.1. The (DSLs) Designated Safeguarding or Deputy Designated Safeguarding Leads (DDSL) at Kelford School who would deal with any related safeguarding matters (including Online Safety are:

- Kari Anson                      Headteacher and DSL
- Catherine Bentley          Deputy Head and DSL
- Carl Haag                      Assistant Headteacher DSDL - Online Safety Lead
- Sharon Wainwright        Assistant Headteacher DDSL
- Kirsty Metcalf              Assistant Headteacher DDSL
- Lisa Atkin                     Post 16 Centre Manager and DDSL
- Collette Gillott              Family Liaison Officer and DDSL

2.7.2. However, Kelford School views that Online Safety is the responsibility of the whole school community and has identified the following groups which have specific responsibilities:

2.7.3. **Nexus MAT Board of Directors** are responsible for the approval of school policies.

### 2.7.4. Senior Leadership Team

The school's senior leaders should:

- Develop and promote an Online Safety culture in school.
- Support the work of the Designated Teacher for Child Protection.
- Provide resources, support and training.
- Ensure the school supports and follows its policies, procedures and systems that are in place to meet GDPR legislation
- Be responsible for the Online Safety of the whole school community.
- Develop opportunities for learning about Online Safety within the curriculum.

### 2.7.5. Designated Safeguarding & E Safety leads. (inc. Headteacher)

The Designated Safeguarding Lead/s should:

- Be the first point of contact for Online Safety in school.
- Develop and maintain Online Safety policies and procedures.
- Understand Online Safety legislation and guidance.
- Promote Online Safety to parents, carers and the wider school community.
- Develop opportunities for learning about Online Safety within the curriculum.
- Keep an up-to-date record of Online Safety incidents.



- Monitor and report on Online Safety incidents.
- Support SLT in following up Online Safety incidents.
- Consult on and approve the removal of online filters
- Support teachers and class teams to liaise with identified parents/carers re. Online Safety

#### **2.7.6. Class Teams and Support Teams:**

Teachers, Teaching Assistants and Support Assistants should:

- Read, understand and help to promote the school's Online Safety policies and guidance.
- Read, understand and follow the school's Acceptable Use Policy (AUP).
- Understand current Online Safety legislation and guidance.
- Model safe and responsible use of ICT.
- Report all Online Safety incidents to the Designated Teacher for Child Protection.
- Develop opportunities for learning about Online Safety within the curriculum.
- Carefully supervise pupils' use of ICT in school.
- Support pupils to understand the ICT Rules.
- Liaise with and support parents/carers re. Online Safety in the home for high risk pupils

#### **2.7.7. Technical Support**

Technicians should:

- Read, understand and help to promote the school's Online Safety policies and guidance.
- Read, understand and follow the school's AUP.
- Understand current Online Safety legislation and guidance.
- Support the school in providing a safe technical infrastructure to support learning and teaching.
- Be responsible for the security of the school's ICT systems.
- Liaise with the Local Authority, partner organisations and service providers.
- Model safe and responsible use of ICT.
- Report all Online Safety incidents to the Online Safety Leader.
- Ensure all passwords are changed every 90 days.
- To risk assess any new technology brought into school.

#### **2.7.8. Pupils**

Pupils should:

- Read, understand and follow the ICT rules.
- Help the school to create Online Safety policies and guidance.
- Learn about the benefits and risks of using ICT the internet and online gaming.
- Use ICT and the internet safely in school and at home.
- Respect the feelings and rights of other people.
- Understand what to do if you feel worried, uncomfortable,



- vulnerable or at risk when using ICT in school or at home.
- Discuss Online Safety in an open and honest way with family and friends.

### 2.7.9. Parents and Carers

Parents and Carers should:

- Help and support the school in promoting Online Safety.
- Read, understand and promote the school's Acceptable Use Policy.
- Learn about the benefits and risks of using ICT and the internet.
- Discuss Online Safety with your children, show interest in how they are using ICT and encourage them to use ICT in a safe and responsible way.
- Model safe and responsible use of ICT at home.
- Discuss your child's use of ICT in school.

## 3. Learning and Teaching

### 3.1. The importance of Internet Use

3.1.1. Internet use is part of the statutory curriculum and is a necessary tool for learning. The Internet is a part of everyday life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience. Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security. The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. Internet access is an entitlement for students who show a responsible and mature approach to its use.

3.1.2. Developing good practice in Internet use as a tool for teaching and learning is essential. Respect for copyright and intellectual property rights, and the correct use of published material should be taught. Whilst the Computing curriculum provides pupils with a whole range of digital skills, because of the cross curricular nature of Internet use, a whole school approach to ICT should be adopted.

3.1.3. The school's Internet access will be designed to enhance and extend education and will include filtering appropriate to the age of the pupils via the Net sweeper filtering system. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use through their PSHE curriculum and through opportunities throughout the range of curricular. In addition, all staff will be responsible for reminding pupils of responsible use prior to any Internet session. Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.

3.1.4. Pupils will be educated in the effective use of the Internet in research.

3.1.5. The ability to use ICT safely and responsibly is important for all our pupils. It



will help them to safely benefit from the opportunities ICT provides.

#### 3.1.6. At Kelford we will:

- Promote Online Safety throughout the curriculum and through a planned programme of whole school activity.
- Provide pupils with relevant Online Safety information and updates e.g. the need to protect personal information, consider the consequences of their actions and the need to check the accuracy and validity of information.
- Remind parents and carers about their responsibilities by asking them to sign an Acceptable Use Policy.
- Model safe and responsible behaviour in our own use of technology in school.

### 3.2. Involving Parents and Carers:

3.2.1. It is important to help all our parents and carers to develop the knowledge, skills and understanding they need to keep themselves and their children safe. At Kelford we will:

- Provide useful links and information on Online Safety in newsletters and on the school website.
- Provide all parents and carers with links to on-line resources
- Provide information, advice and support through termly Parents and Carers meetings
- Provide support and advice for Parents and Carers, particularly those of learners identified as high risk through the Online Safety risk assessments.

### 3.3. Managing ICT Systems and Access:

3.3.1. The school will provide safe and secure access to ICT systems. All ICT hardware and software will be regularly maintained and updated. Virus protection is installed on the school's network. This is activated and kept up-to-date.

3.3.2. Internet access and levels of internet access are managed by the school. All users of ICT will be given a school Acceptable Use Policy to read and understand and will sign a Nexus Acceptable Use Policy (AUP) which links to other Nexus policies which relate to Online Safety and information governance. Users will be made aware of their responsibility for safe and responsible use of ICT and informed that use of the school's ICT systems is monitored and checked. The school has the facility to provide individual access to all pupils using a given log-on. Pupils will be identified for this through the Online Safety risk assessment. Their class teacher will initiate this with the IT Department and retain a copy of this log-on and password. All pupils, whether supervised or working independently, will follow the school's ICT rules. All adults will access the internet using an individual log-on which they will keep secure. All adults will follow the school's AUP. Any administrator passwords for the school's ICT systems will be kept secure and available to a minimum of two adults e.g. School Business Manager and ICT Technician.



3.3.3. The school will take all responsible steps to stop users from accessing inappropriate content. However, it is not possible to guarantee that access to inappropriate content will never happen. The school will regularly audit the ICT use and review the effectiveness of Online Safety policies and practice. The school will review internet access provision and consider new methods for identifying, assessing and minimising risks.

### 3.4. Internet Access

3.4.1. The school uses a filtered internet service. Pupils are set up with 'locked down' internet access and filters are updated both from an external central database and they can also be updated by the school. In the event of a filter prohibiting access to sites or key words prohibiting searches that are deemed appropriate and proper for use in school, the Online Safety lead will be responsible for initial permissions for the removal of blocks which will then be referred to the technician. Logs are kept of all internet access, including any attempts to access blocked sites.

3.4.2. If a user discovers a website with inappropriate (or potentially illegal) content, this should be reported to the DSL (Designated Safeguarding Lead). The school will report potentially illegal content to the filtering provider, Local Authority and CEOP. The school will regularly review all security systems so that they meet the needs of all users in school.

### 3.5. Learning Technologies in School: e-mail

3.5.1. Staff and pupils should use approved e-mail accounts which have been allocated by the school. All approved e-mail accounts are monitored and checked. Staff and pupils will be reminded about the need to send polite and responsible messages, about the dangers of revealing personal information, about the dangers of opening e-mails from unknown senders and opening attachments. Communication between staff and pupils and members of the wider school community should be restricted to school matters. Any inappropriate use of the school e-mail system, or the receipt of any inappropriate messages by a user, should be reported to either the DSL, the Online Safety Co-ordinator or the Data and Systems Manager.

### 3.6. Use of Applications, Images, Video and Sound

3.6.1. Pupils will be taught about safe and responsible behaviours when using software and applications, and when creating, using and storing digital images, video and sound. Digital images, video and sound will only be created using equipment provided by the school. Exceptions will only be made to persons authorised by the Headteacher upon completion of a signed agreement. Digital images, video and sound will not be created without the permission of participants. Images and video will be of appropriate activities. Full names of participants will not be used either within the material or in any accompanying text. All materials will not be published without the permission of participants or, for pupils, participant's parents and carers. Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.



### **3.7. Out of School Events**

3.7.1. Parents and Carers of pupils who attend events beyond the normal school day will be notified prior to the event by letter that photographic images and video footage may be taken which will be beyond the school's control.

### **3.8. Pupils Educated off site**

3.8.1. Pupils who access part of their learning in another educational establishment require staff to follow the guidance and procedures in line with the school's policy and acceptable use agreement. It is the responsibility of Kelford staff members to notify all professionals about the restrictions of publicising digital images and videos for our pupils.

### **3.9. Social Networking, Social Media and Personal Publishing**

3.9.1. Parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking sites provide on-line communities and can connect people with similar or even very different interests. Users can be invited to view personal spaces and leave comments, over which there may be limited control. Blogging, podcasting and other publishing of online content by pupils will take place through regulated learning restrictions. Pupils will not be able to create or post content on websites with public access without adult supervision. Pupils will be taught safe and responsible behaviour in the creation and publishing of online content e.g. pupils will be taught not to reveal personal information.

3.9.2. Staff and pupils will be encouraged to adopt safe and responsible behaviours in their personal use of blogs and social networking sites. Staff should not post personal opinions relating to school matters on blogs or social networking sites and staff are strongly advised not to become 'friends' with any pupil, or their parents or carers.

3.9.3. For responsible adults, social networking sites provide easy to use, free facilities, although advertising often intrudes and some sites may be dubious in content. Pupils should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published.

3.9.4. All staff should be aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. They should be aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

3.9.5. Examples of social media and personal publishing tools include: blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, chatrooms, instant messenger and many others.

3.9.6. The school will control access to social media and social networking sites.

3.9.7. Staff wishing to use Social Media tools with students as part of the curriculum





will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. They will use the school Risk Assessment checklist and will obtain documented consent from the Senior Leadership Team before using Social Media tools in the classroom. Blogs or wikis will be password protected and linked to the school website with approval from the Senior Leadership Team. Members of staff are advised not to run social network spaces for pupil use on an individual basis.

3.9.8. All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

3.9.9. Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites. Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Computer/Internet Use Code of Practice, together with the potential consequences of unacceptable online behaviour both professional and personal.

### 3.10. **Mobile Phones**

3.10.1. Mobile phones will only be used in school with permission from a member of the Senior Leadership Team (SLT). Where staff are required to use a mobile phone for out-of-school or out-of-hours activities, or for contacting pupils or parents, the school mobile phone will be used. Staff will not be expected to use personal mobile phones in any situation where their personal mobile phone number or personal information may be revealed to pupils or parents. Personal mobile phones should not be used to photograph children and young people.

### 3.11. **Staff Use of Personal Devices (mobile phones, iPad, tablets)**

- Staff are not permitted to use their own personal phones or devices for contacting pupils and their families within or outside of the school in a professional capacity.
- Staff will be issued with a school phone where contact with pupils or parents/carers is or may be required e.g. a school trip or out of school learning.
- Mobile phones and devices must be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones or devices must not be used during teaching periods or formal school time e.g. Assemblies unless permission has been given by a member of Senior Leadership Team in emergency circumstances.
- If members of staff have an educational reason to allow pupils to use mobile phones or personal device as part of an educational activity, then it will only take place when approved by the Senior Leadership Team and a risk assessment has taken place.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.



- Staff should not use their own personal devices e.g. laptop, tablet, iPad to deliver lessons or work with pupils, as the school cannot be responsible for the content accessed on such devices.
- Devices loaned to staff by the school e.g. laptops or iPads which are accessed outside of the school network are essentially to support professional activity. These devices are not intended for third party use and members of staff must be aware that they are responsible for the maintenance of confidentiality of school information that may be held on such devices.
- Laptops and other devices loaned to staff are subject to the Laptop/Device Agreement signed by the member of staff.
- If a member of staff breaches the school policy, then disciplinary action may be taken.

### 3.12. **Pupil Use of Personal Devices (mobile phones, iPad, tablets)**

- Kelford School encourages pupils, parents and carers to not send/bring in and personal devices as the school will not be held liable for any loss or damage.
- Mobile phones are not to be used during lesson times unless it is part of the learning activity (e.g. travel training).
- Mobile phones can only be used at breaks and lunchtimes with the permission from a senior member of staff.
- All pupils who bring in personal devices must, inform a staff member, follow the ICT safety rules and the item will be kept secure
- For any pupil found to be in breach of the above may their parents will be informed.
- Mobile phones may be confiscated if a pupil does not abide by the school rules. Parents could be asked to come and collect these phones.

### 3.13. **Visitor Use of Personal Devices (mobile phones, iPad, tablets, laptops)**

- All visitors will be informed that taking photographs of pupils is not permitted and they will be asked to sign a declaration to say they understand this.
- Parents will be asked to sign a Parent and Carer ICT and Online Safety agreement
- Any breach of this policy will be taken very seriously.
- Any use of the internet by a visitor that is in breach of this policy will be discussed with the visitor. Further action could be taken if the matter is not resolved.

### 3.14. **New Technologies**

- New applications are continually being developed based on the Internet, the mobile phone network, wireless, Bluetooth or infrared connections. Users can be mobile using a phone, games console or personal digital assistant with wireless Internet access. This can offer immense opportunities for learning as well as dangers such as a pupil using a phone to video a teacher's reaction in a difficult



situation. The school will keep up-to-date with new technologies and will consider the benefits of these technologies for learning and teaching together with the Online Safety risks. The school will review and update the Online Safety Policy in response to any new technologies and their associated Online Safety risks

### **3.15. The School Website and Facebook page**

- School websites provide opportunities to celebrate pupils' work promote the school and publish resources for projects. Publication of any information online should always be considered from a personal and school security viewpoint. The contact details on the school website will be the school address, email and telephone number. Staff or pupils' personal information must not be published, other than staff name. Subject Leaders will be responsible for ensuring that content relating to their subject areas is accurate, appropriate and up to date. The Headteacher takes overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate. The school website will comply with the school's guidelines for publications including respect for intellectual property rights, policies and copyright.

### **3.16. Publication of Pupil Images and Work**

- The security of staff and pupils is paramount. Images or videos that include pupils should be selected carefully and parent's/carer's permission will be obtained before being electronically published. Pupils' full names will not be used anywhere on the website, particularly in association with photographs without the express permission of parents/carers. Pupils work can only be published with their permission or the parents/carers. Written consent will be kept by the school where pupils' images are used for publicity purposes, until the image is no longer in use. However, this consent can be withdrawn by parents at any time by contacting school. Pupils who are looked after by the authority (LAC) will have not any images published until permission is sought from carers.

### **3.17. Risk Assessment**

- As the quantity and breadth of information available through the Internet continues to grow it is not possible to guard against every undesirable situation. Risks can be considerably greater where tools are used which are beyond the schools control such as most popular social media sites. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot accept liability for the material accessed, or any consequences resulting from Internet use. The school will audit ICT use to establish if the e-Safety policy is adequate and that the implementation of the e-Safety policy is appropriate.



The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to relevant authorities. A risk assessment will be carried out before the introduction of any new technology by the ICT Technicians.

## 4. Online Safety Incidents

### 4.1. Responding to Incidents of Concern

4.1.1. Where there is cause for concern or fear that illegal activity has taken place or is taking place involving the use of computer equipment, the level of response necessary will be determined for the offence disclosed e.g. involving the police. All members of the school community will be informed about the procedure for reporting Online Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc.). The Designated Safeguarding Lead will record all reported incidents and actions taken in the School Online Safety incident log and in any other relevant areas e.g. Bullying or Child Protection log. The Designated Safeguarding Lead must be informed of any Online Safety incidents involving Child Protection concerns, which will then be escalated appropriately. The school will inform parents/carers of any incidents of concerns as and when required. After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required. Where there is cause for concern or fear that illegal activity has taken place or is taking place the school will contact the relevant authorities and escalate the concern to the Police.

4.1.2. All concerns and actions are logged on CPOMS.

4.1.3. If an incident of concern relating to child protection needs to be passed beyond the school, then the Designated Safeguarding Lead will escalate the concern to the Local Authority.

### 4.2. Handling Online Safety complaints

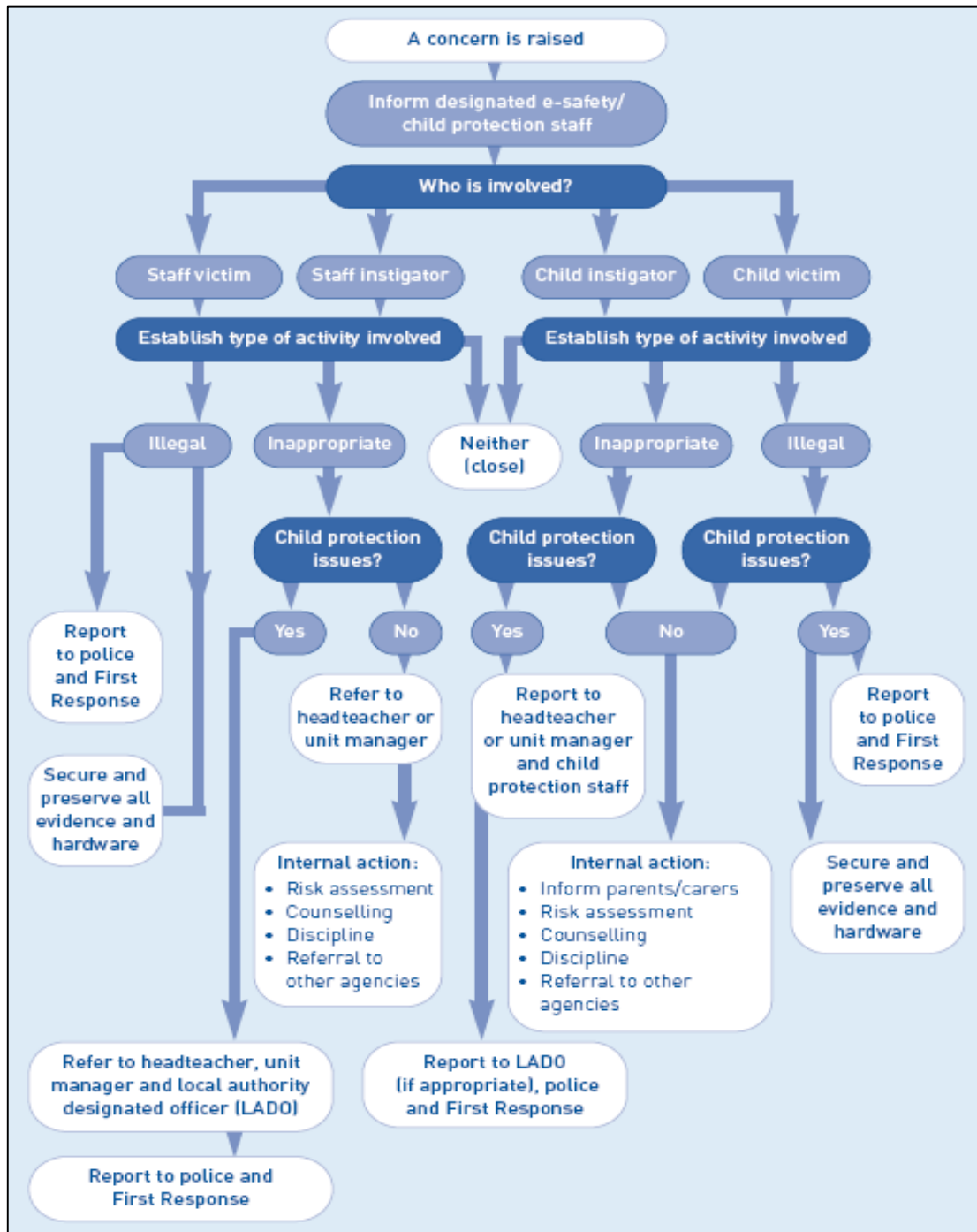
4.2.1. Prompt action will be taken if a complaint regarding irresponsible use is made. The facts of the incident or concern will be established and evidence gathered where possible and appropriate. Online Safety incidents may have an impact on pupils, staff and the wider school community both on and off site and can have civil, legal and disciplinary consequences.

- Complaints about irresponsible use must be reported to the Designated Safeguarding Lead who will be responsible for handling incidents.
- Any complaint about staff misuse must be referred to the Headteacher. Pupils and parents/carers will be informed of the complaints procedure.



- All e–safety complaints and incidents will be recorded by the school, including any actions taken via CPOMS
- Parents/Carers and pupils will need to work in partnership with the school to resolve issues.
- All members of the school community should be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- All members of the school community will be reminded about safe and appropriate behaviour online (in and out of school) and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.
- There may be occasions when the police must be contacted. This is a decision the Headteacher or Designated Safeguarding Lead will make when the all the facts are presented.

## 5. Flowchart for managing an Online Safety incident



## 6. Cyberbullying

6.1. Cyberbullying can be defined as “The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone” DCSF 2007.

6.2. Many young people and adults find that using the internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. When children are the target of bullying via mobiles phones, gaming or the Internet, they can often feel very alone, particularly if the adults around them do not understand cyberbullying and its effects. A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety.

6.3. It is essential that our young people, school staff and parents and carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

6.4. Where bullying outside school (such as online or via text) is reported to the school, it will be investigated and acted on.

6.5. Although bullying in itself is not a specific criminal offence in the UK, it is important to bear in mind that some types of harassing or threatening behaviour or communications could be a criminal offence, for example under the Protection from Harassment Act 1997, the Malicious Communications Act 1988, the Communications Act 2003, and the Public Order Act 1986. If the school feels that an offence may have been committed, advice from the police will be sought. DfE and Childnet have produced resources and guidance that can be used to give practical advice and guidance on cyberbullying: <http://www.digizen.org/cyberbullying>

- Cyberbullying on or off site (along with all other forms of bullying) of any member of the school community will not be tolerated. The school has a comprehensive anti-bullying policy.
- Pupils can report cyberbullying to any member of staff. The Designated Safeguarding Lead must be informed of any reported cyberbullying so that incidents can be recorded and appropriate procedures followed.
- Staff should report any incidents of cyberbullying they experience to a member of the SLT.
- All incidents of cyberbullying reported to the school will be recorded.
- There are clear procedures in place to support anyone in the school community affected by cyberbullying.
- There are clear procedures in place to investigate incidents or

allegations of cyberbullying.

- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, contacting the service provider and police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's Online Safety ethos.
  - Sanctions for those involved in cyberbullying may include:
    - The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
    - Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti- bullying, behaviour policy or Computer/Internet Use Code of Practice.
    - Parent/carers of pupils will be informed.
      - The Police will be contacted if a criminal offence is suspected.

6.6. Keeping children safe in education also highlights the risk posed to learners through the use of online technologies with regards to Child sexual exploitation; radicalisation; sexual predation. Annual staff safeguarding and Online Safety training serve to ensure that staff are aware and vigilant of these risks and the potential signs of a young person who is vulnerable to or suffering online abuse of any kind.

6.7. The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- content: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;
- contact: being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and
- conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.
- This is reflected in the class and individual Online Safety risk assessments completed and reviewed annually for all pupils.

## 7. Communication Policy Pupils

7.1. Online Safety will be introduced and discussed with pupils mainly through the computing and PSHE curriculum but also at opportune moments throughout via embedded learning. Posters displaying Online Safety rules are available for display in every classroom. Reminders about responsible



and safe use should precede lessons where computers and the Internet are being used.

- All users will be informed that network and Internet use will be monitored.
- An e–Safety training programme will be established across the school to raise the awareness and importance of safe and responsible internet use amongst pupils.
- Pupil instruction regarding responsible and safe use will precede Internet access.
- An e–Safety module will be included in the PSHE, Citizenship and/or computing programmes covering both safe school and home use.
- Online Safety rules will be posted in all rooms with Internet access.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.
- Particular attention to Online Safety education will be given where pupils are considered to be vulnerable.

## 7.2. Staff

7.2.1. The School e–Safety Policy will only be effective if all staff subscribe to its values and methods.

7.2.2. All staff must understand that the rules for information systems misuse are specific and that instances resulting in disciplinary procedures and dismissal have occurred.

7.2.3. If a member of staff is concerned about any aspect of their ICT or internet use either on or off site, they should discuss this with their line manager or Online Safety coordinator to avoid any possible misunderstanding.

7.2.4. Induction of new staff includes a discussion about the school e–Safety Policy.

- The e–Safety Policy will be formally provided to and discussed with all members of staff.
- To protect all staff and pupils, the school will implement a Code of Practice which all users must agree to and sign.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be available for all members of staff as required.
- Staff nominated to monitor ICT use will be supervised by the Headteacher, Deputy Headteacher (Safeguarding) and Assistant Headteacher (Online Safety) and have clear procedures for reporting issues.
- All members of staff will be made aware that their online

conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or school into disrepute, or if something is felt to have undermined confidence in their professional abilities.

## 8. Transitions

- 8.1. The importance of online safety will be covered as part of the school's admissions meeting. The Parent and Carer ICT and Online Safety agreement will be included in the pack.

## 9. Parental Support

- 9.1. Internet use in pupils' homes is increasing rapidly, encouraged by low cost access and developments in mobile technology. Unless parents are aware of the dangers, pupils may have unrestricted and unsupervised access to the Internet in the home. Parents will be advised of the importance of Online Safety and of suitably, helpful organisations.

- Parents' attention will be drawn to the school e-Safety Policy in newsletters, the school prospectus, on the school website.
- A partnership approach to Online Safety at home and at school with parents will be encouraged. This may include offering parent & carer workshops with demonstrations and suggestions for safe home Internet use, or highlighting e-Safety at other attended events e.g. parent & carers day and sports days.
- Parents & carers will be requested to sign an ICT and e-Safety agreement.
- Parents & carers will be encouraged to read the school Code of Practice for pupils and discuss its implications with their children.
- Information and guidance for parents & carers on e-Safety will be made available to parents.
- Interested parents & carers can contact the school if they require further help and support.

### 9.2. Communication of Policy Pupils

- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that Internet use will be monitored
- All pupils will follow school ICT rules

### 9.3. Staff

- All staff will be given the School Online Safety Policy during their induction and its importance explained.
- All staff will receive a copy of the Online Safety policy.
- All staff will read and sign the ICT Acceptable Use Policy (AUP)
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

## **APPENDIX 1**

### **Online Safety Contacts and References**

CEOP (Child Exploitation and Online Protection Centre):

[www.ceop.police.uk](http://www.ceop.police.uk) Childline: [www.childline.org.uk](http://www.childline.org.uk)

Childnet: [www.childnet.com](http://www.childnet.com)

Children's Safeguards Team: [www.kenttrustweb.org.uk?safeguards](http://www.kenttrustweb.org.uk?safeguards)

Click Clever Click Safe Campaign:

<http://clickcleverclicksafe.direct.gov.uk>

Cybermentors: [www.cybermentors.org.uk](http://www.cybermentors.org.uk)

Digizen:

[www.digizen](http://www.digizen)

[.org.uk](http://www.digizen.org.uk)

GDPR:

<https://www>

[.eugdpr.org/](https://www.eugdpr.org/)

Internet Watch Foundation

(IWF): [www.iwf.org.uk](http://www.iwf.org.uk)

Kidsmart:

[www.kidsmart.org.uk](http://www.kidsmart.org.uk)

NSPCC: [www.nspcc.org.uk](http://www.nspcc.org.uk)

Safer Internet:

[www.Saferinternet.or](http://www.Saferinternet.or)

[g.uk](http://www.Saferinternet.org.uk) Teach Today:

[http://en.teachtoday.](http://en.teachtoday)

[eu](http://en.teachtoday.eu)

Think U Know website: [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk)

Virtual Global Taskforce — Report Abuse: [www.virtualglobaltaskforce.com](http://www.virtualglobaltaskforce.com)

Information Commissioner's Office – Data Protection:

[www.ico.gov.uk/](http://www.ico.gov.uk/)

### **Other Legislation on Computer Misuse Act 1990**

This Act makes it an offence to:

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

### **Data Protection Act 1998**

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

unlawfully. The Act states that person data must be:

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

### **Freedom of Information Act 2000**

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

### **Communications Act 2003**

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

### **Malicious Communications Act 1988**

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

### **Regulation of Investigatory Powers Act 2000**

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

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

### **Trade Marks Act 1994**

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

### **Copyright, Designs and Patents Act 1988**

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

### **Telecommunications Act 1984**

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

### **Criminal Justice & Public Order Act 1994**

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

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

### **Racial and Religious Hatred Act 2006**

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

### **Protection from Harassment Act 1997**

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

occasions.

### **Protection of Children Act 1978**

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

### **Sexual Offences Act 2003**

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

### **Public Order Act 1986**

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

### **Obscene Publications Act 1959 and 1964**

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

### **Human Rights Act 1998**

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

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

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and

obligations, which arise from other relevant legislation.

**The Education and Inspections Act 2006**

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

**The Education and Inspections Act 2011**

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data. (see template policy in these appendices and for DfE guidance - [http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviour\\_policies/f0076897/sc\\_reening-searching-and-confiscation](http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviour_policies/f0076897/sc_reening-searching-and-confiscation))

**The Protection of Freedoms Act 2012**

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

**The School Information Regulations 2012**

Requires schools to publish certain information on its website: <https://www.gov.uk/guidance/what-maintained-schools-must-publish-online>

**Serious Crime Act 2015**

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

## Appendix B

### ICT Acceptable Use Policy

This policy is designed to make all staff aware of their responsibilities when using any form of ICT<sup>i</sup> in school. Please read thoroughly.

- I will only use ICT and any related technologies for professional purposes or for uses deemed 'reasonable' by the school.
- I will comply with ICT security policies and not disclose any passwords provided to me by the school.
- I will ensure that all electronic communications with children, young people and adults are appropriate to my professional role.
- I will not give out my own personal details, such as a mobile phone number and personal e-mail address to children and young people.
- I will only use approved e-mail system(s) for work.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off-site or accessed remotely. Personal data can only be taken off-site or accessed remotely when authorised by the school.
- I will not install or use any ICT hardware or software without prior permission.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of children and young people will only be taken, stored and used for professional purposes in line with the school's Online Safety policy.
- I understand that all my use of the internet and other related technologies can be monitored and can be made available, on request, to the school.
- I will respect copyright and intellectual property rights.
- I will ensure that my on-line activity, both work-related and in private environments, will not bring my professional role into disrepute.
- I will support and promote the Acceptable Use Policy (AUP) and help children, young people and adults to be safe and responsible in their use of ICT and related technologies

---



<sup>i</sup> Information and Communications Technology
















## Appendix C

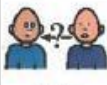
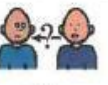





### Pupil Use of ICT






For the purposes of both instruction/direction and developing understanding the school will use adapted written/visual 'rules' in line with those listed below for E-safety and the use of ICT in line with the communicative needs. All pupils will follow the SMART rules & Pupils on the orange pathway and anyone identified as high risk with regards to Online Safety will also learn the 10 golden rules.









**Kelford e-safety rules: Be SMART**








**S**  :       
 Safe : Keep information about you safe.

**M**  :        
 Meet : don't meet strangers from the internet.

**A**  :        
 Ask : Ask an adult when you want to  
 go on the computer or the internet.

**R**  :      
 Remember : keep your passwords secret.

**T**  :        
 Tell: Tell an adult if something upsets you're online.

**Kind:**  **Be** **A**       
 Kind: Be a good friend when you're online.



# 10 e or e-safety rules: 10 Golden Rules.



**1** Do not use passwords safely.

**6** Do not report to CEOP.

**2** Do not check your messages.

**7** Do not be a good friend online.

**3** Stop and think before you post.

**8** Be careful what you say when online.

**4** Remember people are not always who they seem to be.

**9** Don't break the law online.

**5** If something upsets you online.

**10** What you do online is monitored to protect your life.

## Appendix D

### Photo Permissions

At Kelford School, we sometimes take photographs and videos of pupils. We use these in the school's prospectus, in newsletters, on the school's website, within presentations showcasing the work of the school and on display boards around school.

We would like your consent to take photos and videos of your child, and use them in the ways described above. If you're not happy for us to do this, that's no problem – we will accommodate your preferences.

Please tick the relevant box(es) below and return this form to school.

I am happy for the school to take photographs and videos of my child.	<input type="checkbox"/>
I am happy for photos and videos of my child to be used on the school website and Facebook.	<input type="checkbox"/>
I am happy for photos of my child to be used in the school prospectus.	<input type="checkbox"/>
I am happy for photos and videos of my child to be used in internal displays and presentations.	<input type="checkbox"/>
I am happy for photos and videos of my child to be included in external presentations.	<input type="checkbox"/>
I am happy for photos of my child to be included in the school newsletter.	<input type="checkbox"/>
I am happy for photos and videos of my child to be used in the messaging app, SchoolZine, which is used to send messages and alerts to families and staff.	<input type="checkbox"/>
I am happy for my child to be part of the yearly class photo's which will be available for families to purchase.	<input type="checkbox"/>
<b>I am NOT happy for the school to take or use photos and videos of my child.</b>	<input type="checkbox"/>

If you change your mind at any time, you can let us know by emailing [kelfordschool@nexusmat.org](mailto:kelfordschool@nexusmat.org) or by calling the school on 01709 512088, or just popping in to the school office.

If you have any other questions, please get in touch.

#### **Why are we asking for your consent?**

You may be aware that new data protection rules (GDPR) came in from May 2018. To ensure we are meeting the new requirements, we need to seek your consent to take and use photos and videos of your child. We really value using these to be able to showcase what pupils do in school and show what life at our school is like to others, so we would appreciate you taking the time to give consent.

<b>Parent or Carer's Signature:</b>	
<b>Date:</b>	

## **Appendix E**

### **Online Safety Incident Log:**

Date of incident:	
Person reporting:	
Website of incident:	
Copy of screen/evidence saved to:	
Location of incident:	
Computer number:	
Details:	
Passed to:	
Action taken:	