Scope of the Policy

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

This policy is to be read in conjunction with the school's Child Protection and Safeguarding, Anti-Bullying, Behaviour, Data Protection and Whistleblowing policies.

The Education and Inspections Act 2006 empowers Head Teachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other E-Safety incidents covered by this policy, which may take place outside of Ingham Primary School, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

Ingham Primary School will deal with such incidents within this policy (and associated behaviour and anti-bullying policies) and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that takes place outside of school.

1. Introduction

At Ingham Primary School we understand the responsibility to educate our pupils on E-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom. We do this by:

- Having a framework for teaching internet skills
- Providing opportunities within a range of curriculum areas to teach about E-Safety
- Educating pupils on the dangers of technologies that maybe encountered outside school
- Teaching pupils the impact of cyberbullying and how and where to seek help if they are affected by any form of online bullying i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline.

2. Assessing risks

The school will:

- Take all reasonable precautions to ensure that users access only appropriate material. However, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor LCC can accept liability for the material accessed, or any consequences of Internet access.
- Audit ICT provision to establish if the E-Safety policy is adequate and that its implementation is effective.
- Regularly review methods to identify, assess and minimise risks. When needed (for example, when new equipment arrives) a risk assessment, in collaboration with ARK, will be carried out.
- Make sure all users are aware of the procedures for reporting accidental access to inappropriate materials (see Appendix 2 for flow chart). The breach must be immediately reported to the E-Safety lead. After investigation, if deemed necessary, the incident will be logged on CPOMS. This will be supported by the filtering system used (Securly) where email notification is received by the E-Safety Leader and Head Teacher informing them of the day, time and device used for the access of inappropriate internet content.

3. Managing Internet Access and Filtering

3.1. Information system security

- School ICT systems capacity and security will be reviewed regularly.
- All staff, students and parents of students will be informed that Internet activity may be monitored in order to ensure as much as possible that users are not exposed to illegal or inappropriate websites, and to ensure as much as possible that users do not actively seek access to illegal or inappropriate websites
- The Computing Lead, E-Safety Leader and ARK IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Head Teacher.

- Security strategies and updates will be discussed, when needed, with LCC and IT providers.
- Regular checks will be made to ensure that the filtering methods selected are appropriate, effective and reasonable.

3.2. Virus Protection

At Ingham we use Avast Business CloudCare anti-virus software. All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. IT Support will be responsible for ensuring this task is carried out, and will report to the Head Teacher if there are any concerns.

Staff must make sure that:

- Pupils are not permitted to download programs or files on school-based technologies without seeking prior permission.

3.3. E-mail

- At Ingham we use Avast Business CloudCare software that prevents any infected email being sent or received by the school.
- It is the responsibility of each account holder to keep their password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced.
- Pupils may only use school approved accounts on the school system and only under teacher supervision for educational purposes.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not give personal details of themselves or others in e-mail communication, or arrange to meet anyone or send anything offensive.
- All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly, use of personal email addresses for work purposes is not permitted.

3.4. Use of the Internet

- Younger children's internet use will be supervised through adult-led activities. As children move through key stage 2 their internet use will become more independent. They will be taught procedures if problems occur.
- Staff will preview any recommended sites before use.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

3.5. The Internet and learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils with online activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils should be taught, and regularly reminded, to be aware of the dangers of using the internet and what to do if there is a problem or they are aware of misuse.
- If staff or pupils discover an unsuitable site, it must be reported to the E-Safety Leader.

3.6. Publishing pupil's images and work

- Pupils' full names will not be used anywhere on the Web site, Facebook or Class Dojo ~~or Blog~~, particularly in association with photographs.
- The school permits the appropriate taking of images by staff and pupils with school equipment as part of the children's activities and learning.
- Written permission is obtained from parents or carers regarding the use of photographs of pupils on the school Web site, Facebook and Class Dojo. ~~and blogs~~
- Pupil's work will only be published online platforms using the child's first name.
- Where services are "comment enabled", comments are to be monitored by the class teacher/administrator and brought to the attention of the head teacher if necessary.
- Appendix 1 details specific technology and use with reference to children's photographs.

3.7. Social networking and personal publishing

- Ingham Primary School is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community.
- The school will block/filter access to social networking sites for pupils.
- Pupils will be told never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.
- Pupils are asked to report any incidents of bullying (including cyber bullying) to the school.

The following social media services are permitted for use within Ingham Primary School and have been appropriately risk assessed; should staff wish to use other social media, permission must first be sought via the E-Safety Leader who will advise the Head Teacher for a decision to be made. Any new service will be risk assessed before use is permitted.

- ClassDojo – used by the school as a communication service with parents of the school
- Facebook – used by the school as a broadcast service
- First names only will be used on Class Dojo
- Photos used on broadcast services will not be named; parental permission for broadcast services (including the school website) is different to those for communication within the school community (for example: newsletters). Staff using broadcast services must check that appropriate permission has been given before posting

3.8. Managing emerging technologies (see also 4.4)

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

3.9. Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018

3.10. Password Security

- Use only your own personal log on details, account IDs and passwords and do not allow them to be used by anyone else. In particular, children must not have access to any staff logins.

4. Policy Decisions

4.1. Authorising Internet access

- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school. Parents will be asked to sign and return a consent form.
- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g. on school website, Facebook)

- The school will keep a record of all staff and pupils who are granted internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.

4.2. Handling E-Safety complaints (see Appendix 3)

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Head Teacher.
- If a criminal offence has been committed, whether by a pupil or a member of staff, it is essential that the police are consulted at the earliest opportunity
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Parents and pupils will need to work in partnership with staff to resolve issues.

4.3. Enlisting parents' support

- Parents' attention will be drawn to the School E-Safety Policy through the school web site, which includes signposts to useful websites to support parents in delivering the E-Safety message.
- Internet issues will be handled sensitively, and parents will be advised accordingly.

4.4. Mobile Technologies

Mobile technology devices may be school owned/provided or personally owned (smartphone, tablet, laptop – or other technology that has the capability of utilising the school's wireless network). This device then has access to the wider internet, which includes cloud-based services such as email and data storage. All users should understand that the primary purpose of mobile technology in a school context is educational. Ingham Primary School allows:

	School Devices			Personal Devices		
	School owned for single user	School owner for multiple users	Authorised device (such as laptops for pupil home use during lockdown)	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	No	Yes	Yes
Full network access	Yes	Yes	Usually Yes – but could have limited functions / access	N/A	No	No
Internet only	No	No	No	NN/A	Yes	Yes

4.5. Key responsibilities of individuals

Pupils should:

- With guidance, increasingly develop their own set of safe behaviours to guide them whenever they are online and at the start of each academic year, be part of a whole class acceptable use policy agreement.
- Report any incidents of ICT misuse within school to a teacher
- Seek help or advice from a teacher, or trusted adult, if they experience problems when online, or if they receive or view any content or contact which makes them feel uncomfortable in any way.
- Communicate with their parents or carers about internet safety issues, and keep any rules for safe internet use in the home.

E-Safety Leader should:

- Keep up to date with the latest risks to children whilst using technology; become familiar with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Head Teacher.
- Advise the Head Teacher, governing body on all E-Safety matters.
- Engage with parents and the school community on E-Safety matters at school and/or at home.
- Liaise with the local authority, IT technical support and other agencies as required.
- Ensure staff know what to report and ensure there is an appropriate audit trail.
- Ensure any technical E-Safety measures in school (e.g. Internet filtering software) are fit for purpose through liaison with the local authority and/or ICT Technical Support.
- Be aware of any reporting function with technical E-Safety measures, i.e. internet filtering reporting function; liaise with the Head Teacher and responsible governors to decide on what reports may be appropriate for viewing.

Technical Support Staff will ensure that:

- The IT technical infrastructure is secure; this will include checking that:
    - Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
    - Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
    - Any E-Safety technical solutions such as Internet filtering are operating correctly.
    - Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the E-Safety Leader and Head Teacher.
    - Passwords are applied correctly to all users regardless of age. Passwords for staff will be a minimum of 8 characters.

Governors should:

- Review this policy every three years and in response to any E-Safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure E-Safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.
- Have overall responsibility for Safeguarding and another for the governance of E-Safety at the school who will:
    - Keep up to date with emerging risks and threats through technology use.
    - Receive regular updates from the Head Teacher in regard to training, identified risks and any incidents.
    - Report back to the Governing Body where appropriate

Head Teacher:

Reporting to the governing body, the Head Teacher has overall responsibility for E-Safety within our school. The day-to-day management of this will be delegated to a member of staff: the E-Safety Leader.

The Head Teacher will ensure that:

- E-Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team and governing body, parents.
- The governing body is informed of the issues and the policies.
- The designated E-Safety Leader has had appropriate CPD.
- All E-Safety incidents are dealt with promptly and appropriately.
- Appropriate funding is allocated to support internet safety activities throughout the school, for both the technical infrastructure and Inset training for staff.

- Internet safety is promoted across the curriculum.

Staff will ensure that:

- All details within this policy are understood. The Staff Acceptable Use section of the Staff Handbook has been read and understood. If anything is not understood it should be brought to the attention of the Head Teacher.
- Any E-Safety incident is reported to the E-Safety Leader (and an E-Safety Incident report is made – using CPOMS if a pupil is involved), or in their absence, to the Head Teacher. If staff are ever unsure, the matter is to be raised with the E-Safety Leader or the Head Teacher to make a decision.
- The reporting flowcharts contained within this E-Safety policy are fully understood.

Appendix 1

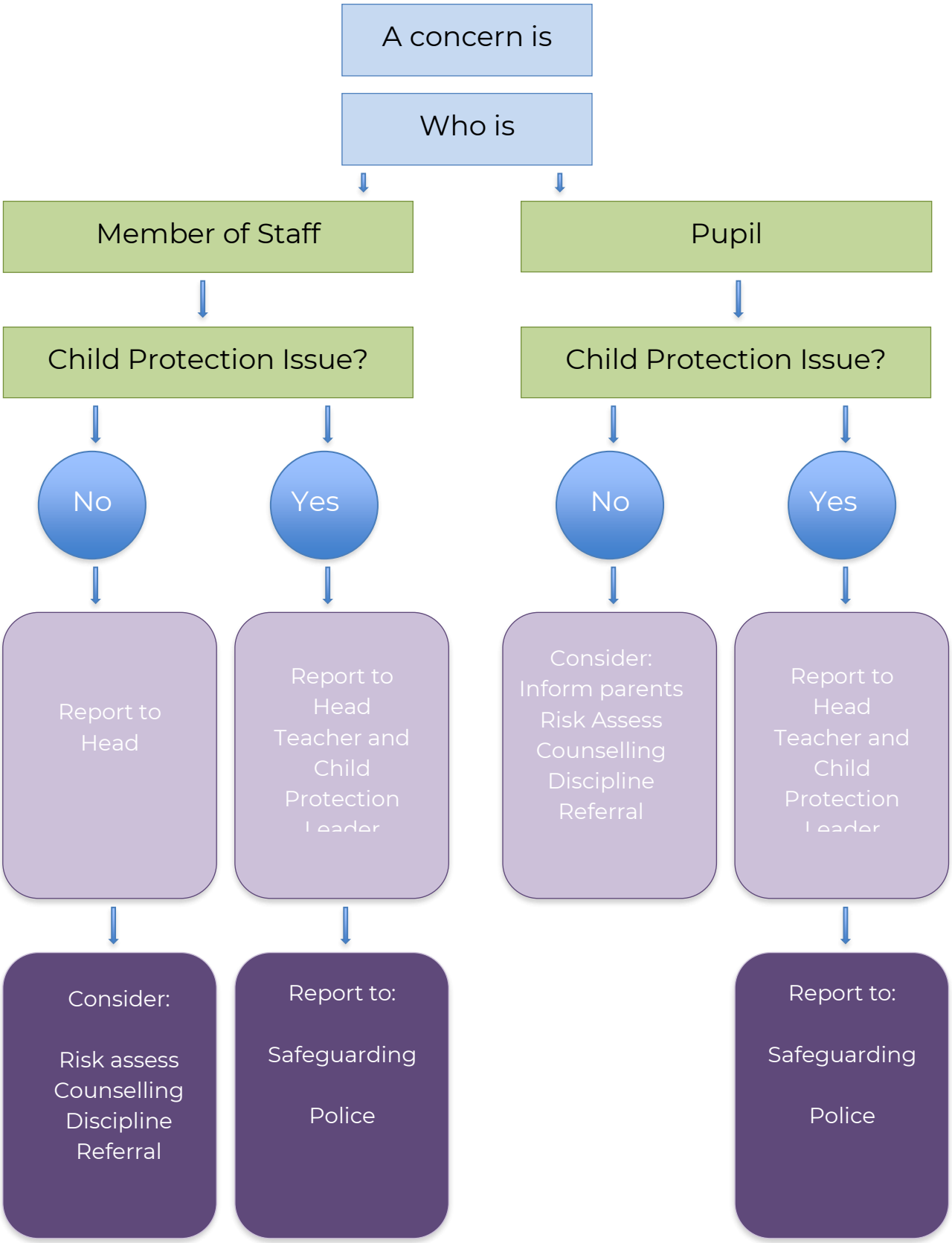
Storage and use of school photographs

Ingham Primary School regularly takes photos of children involved in different learning opportunities throughout the year. These may be in different forms, stored in different places and taken on different devices. Below is a list of devices, locations, use and permission which the school uses pupil photographs

Device or software	Location	Permissions	Access	Reasons
School website	Nexcess Cloud server	Parental permission given for external use	Through Content Management System which is password secured	Broadcast information about the school to wider audience
ClassDojo	ClassDojo Servers	Parental permission as per internal use.	Password protected accounts for staff and parents that the school have approved. (Updated annually)	To communicate information and celebrate achievement within the school community.
School cameras (still and video)	Memory cards	/		
Staff laptops	Shared drive or individual drive (H:)	/	Drives accessed through logins	
iPads	Photographs stored in 2 locations 1. on the iPad 2. Google Drive	/	Google Drive is password protected.	Google Drive allows photos to be shared across multiple iPads for shared learning opportunities.
Cloud Storage: Google Drive (Google) One Drive (Microsoft)	Google/Microsoft Servers	/	Password protected access	Reduce need for internal storage capacity. Allow for easy transfer of files between staff
Home cameras or camera phones	Should not be used in school to take photographs			

Appendix 2

Inappropriate Activity Flowchart



If you are in any doubt, consult the Head Teacher, Child Protection Leader or Safeguarding

Appendix 3

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

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

• Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.

• Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.

• It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).

• Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)

• Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:

o Internal response or discipline procedures
o Involvement by Local Authority
o Police involvement and/or action

• If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

o incidents of 'grooming' behaviour
o the sending of obscene materials to a child
o adult material which potentially breaches the Obscene Publications Act
o criminally racist material
o promotion of terrorism or extremism
o offences under the Computer Misuse Act 2022 (for example: online grooming, pornography, promotion of extremism, cyber-crime, offensive information that may bring the school into disrepute, etc)
o other criminal conduct, activity or materials

• Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

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

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

Students/Pupils Incidents	Refer to class teacher	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering/security etc.	Inform parents/carers	Removal of network/internet access rights	Warning	Further sanction e.g. detention/exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		X	X					
Unauthorised use of non-educational sites during lessons	x							
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device		x			x			
Unauthorised/inappropriate use of social media/ messaging apps/personal email		x			x			
Unauthorised downloading or uploading of files		x						
Allowing others to access school/academy network by sharing username and passwords		x						
Attempting to access or accessing the school/academy network, using another student's/pupil's account		x						
Attempting to access or accessing the school/academy network, using the account of a member of staff		x						
Corrupting or destroying the data of other users		x			x			
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		x			x			
Continued infringements of the above, following previous warnings or sanctions		x			x	x	x	x
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		x			x	x		
Using proxy sites or other means to subvert the school's filtering system		x			x	x		
Accidentally accessing offensive or pornographic material and failing to report the incident		x			x	x		
Deliberately accessing or trying to access offensive or pornographic material		x			x	x	x	x
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		x	x	x	x	x	x	x

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