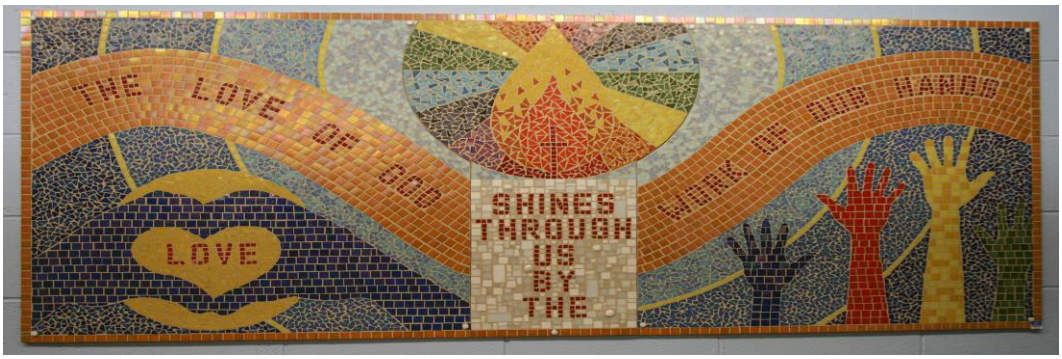
Norley CE Primary School



E-Safety Policy

We are a church school where education is nourished through the teachings of Jesus Christ, enabling each child to fulfil their potential and which reflects our commitment to academic excellence.

We want our children to celebrate and appreciate diversity, fostering qualities that encourage every child to have aspiration for a society in which every individual is cherished.

With our Christian belief at its heart, we work in partnership with each other, families, the church, the local and wider community to create a stimulating and caring environment, where everyone is welcomed, nurtured and empowered.

Christian values directly inspire and influence the children to recognise their self-worth and flourish, enabling them to make the right choices that will continue to shape their lives

You are the light of the world. A city built on a hill cannot be hidden. No one after lighting a lamp puts it under the bushel basket, but on the lamp stand, and it gives light to all in the house. In the same way, let your light shine before others, so that they may see your good works and give glory to your Father in heaven.
(Matt. 5:14-16)

E-Safety Policy

Introduction

E-Safety encompasses the use of new technologies, internet and electronic communications such as Learning Platforms, mobile phones, Video Conferencing, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their on line experience.

The school's e-safety policy will operate in conjunction with other policies including those for Student Behaviour, Bullying, Curriculum, Data Protection and Security, Acceptable Use and Communication Policy. E Safety also relates to the School Safeguarding Policy.

E-Safety depends on effective practice at a number of levels:

- Responsible ICT (Information & Communication Technologies) use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from an approved Internet Service Provider using suitable filtering.
- National Education Network standards and specifications.

Our e-Safety Policy and its implementation is updated on an annual basis. Our e-Safety School Policy has been written in conjunction with staff at school, building on the Cheshire e-Safety Policy and government guidance. It has been agreed by senior management and approved by governors. It will be shared with parents/carers.

Our e-Safety Coordinator is:

- Mrs Kelly

The coordinator works closely with the Local Authority (LA) ICT support service technicians and the Head teacher of the School.

Key LA contacts:

- Child Protection Services
- Primary ICT Adviser

Preventing Extremism and Radicalisation

Our preventing extremism and radicalisation policy is intended to provide a framework for dealing with issues relating to vulnerability, radicalisation and exposure to extreme views. We recognise that the internet and in particular social media are used to radicalise and recruit young people. This policy should be read in conjunction with our Preventing Extremism and Radicalisation policy and the Home Office publication 'How Social Media is used to encourage travel to Syria and Iraq- briefing note for schools.'

In the same way teachers are vigilant about signs of possible physical or emotional abuse in any of our pupils, any concerns for the safety of a specific young person at risk of radicalisation are dealt with using the schools safeguarding procedures. We have a Prevent lead who can also provide support.

Teaching and learning

Why Internet use is important

- The Internet is an essential element in 21st century 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.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning

- The school Internet access will be designed expressly for pupil and family use and will include filtering appropriate to the age of pupils.
- Pupils and families will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Internet Access

i. Information system security

- School ICT systems and security will be reviewed regularly. *(Please refer to Appendix 2)*
- Virus protection will be installed on every computer and will be set to update automatically at least every week if not daily
- We have adopted Cheshire West and Cheshire's security standards

ii. E-mail

- Pupils may only use approved e-mail accounts on the school system. The School does not permit individual pupils to have their own email accounts. Accounts are set up on a class basis.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

iii. Published content and the school web site

- The contact details on the Web site should be the school's address, e-mail and telephone number. Staff or pupils' personal information will not be published.

- The head teacher will take overall editorial responsibility for each website in conjunction with the ICT coordinator and link ICT Governor and ensure that content is accurate and appropriate.

iv. Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. *Please see Understanding Images, Appendix 3 for guidance on how to do this.*
- Pupils' full names will not be used anywhere on the Web site or Blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.

v. Social networking and personal publishing

- The school will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents may be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

vi. Managing filtering

- The school will work with the LA and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the e-Safety (ICT) Coordinator. The Local Authority, as the Internet Service Provider, includes filtering at a County level. If sites are blocked there is a mechanism to release sites on approval by the Advisory team. Where schools find sites or content that is inappropriate they should contact Help Desk on 01244 97400 and ask for the site to be blocked.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. Please see appendix 2.

vii. Managing videoconferencing

- Currently the School does not engage in video-conferencing. Video conferencing is very resource heavy and can have a significant impact upon the performance of the network. Technologies such as Skype may be considered appropriate for home use, are not to be encouraged within the schools' network. Learning platforms are likely to incorporate simple point to point video conferencing as part of their communication tools. However the following guidance would be adhered to if this facility became available:
- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupils' age.

viii. Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in the 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. Pupils are not allowed to bring mobile phones into school.
- Staff will not use personal equipment or non school personal electronic accounts when contacting students. The school phone will be used where contact with pupils is required.

ix. Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation 2018. See reference to General Data Protection Regulation (GDPR) Policy

Policy Decisions

i. Authorising Internet access

- All staff must read and sign the 'Staff Information Systems Code of Conduct' before using any school ICT resource.
- All students and their parents must read and agree to the 'Students' Safety Rules'. This will be issued to parent with the each school's Home School Agreement and Parents will be asked to agree to and return a consent form with respect to the 'Students' Safety Rules'.
- The school will keep a central 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. It is the head teacher's responsibility to ensure that the record is kept up to date so that it can be easily referred to.
- Within the Primary school access to the Internet will be supervised. Lower down the school access will be to specific, approved on-line materials.

ii. Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the School nor the local authority can accept liability for the material accessed, or any consequences of Internet access.
- The school will regularly audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

iii. Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff/ Headteacher
- Any complaint about staff misuse must be referred to the headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures and referred to the Headteacher as Desgnated Safeguarding Person or the School. Pupils and parents will be informed of the complaints procedure and the School Complaints Policy will be followed.

- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

iv. Communications Policy

Introducing the e-safety policy to pupils

- E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year.
- Pupils will be informed that network and Internet use will be monitored.

Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained. A copy will also be held in the central policy files – Curriculum Policy files
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Enlisting parents' support

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.

E-Safety Policy	
Review Frequency:	Annual
Reviewed by:	FGB on behalf of Curriculum & Community Committee 16th June 2020
Head Teacher approval signature:	*Helen Kelly*
Head Teacher approval date:	17/06/2020
Chair of Governing Body approval signature:	*Paul Corbishley*
Chair of Governing Body approval date:	17/06/2020
Date of next review:	16th June 2021

Appendix 1: Internet use - Possible teaching and learning activities

Activities	Key e-safety issues
Creating web directories to provide easy access to suitable websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.
Using search engines to access information from a range of websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.
Exchanging information with other pupils and asking questions of experts via e-mail.	Pupils should only use approved e-mail accounts. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. The Learning Platform.
Publishing pupils' work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils' names and other personal information should be omitted.
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name.
Communicating ideas within chat rooms or online forums.	Only chat rooms contained with the schools Learning Platform and linked to educational use and that are moderated should be used. Access to other social networking sites should be blocked. Pupils should never give out personal information.
Audio and video conferencing to gather information and share pupils' work.	Pupils should be supervised. Only sites that are secure and need to be accessed using an e-mail address or protected password should be used.

Appendix 2

Considerations around access to data from, into and within the school are as follows:

1. Where a school is part of the Cheshire Managed Internet Service network then external security to and from the school is managed by firewalls administered by the Cheshire Managed Internet Service.

2. Additional protection is provided by filtering services for web traffic and external email traffic which are managed by the Cheshire Managed Internet Service. Where a school has a concern that filtering is not blocking inappropriate websites it is their responsibility to contact the Cheshire Managed Internet Service Help Desk to report the website.

3. Where a school buys into a third party ISP service then generally the responsibility to provide firewalls and filtering services is with the schools.

4. School should take responsibility for deciding who is allowed access to data within and external to the school through the use of an authentication policy (user identification and passwords need to be issued and managed)

5. It is the school's responsibility to ensure that the security of any wireless networks is set to block unauthorised access.

6. It is good practice to set screen savers to engage after a maximum of 20 minutes which **require the user to log back in** when deactivated. This helps maintain security of systems by minimising the risk of computers being left logged on for extended periods of time and enabling user accounts to be abused by unauthorised users.

7. Virus protection should be installed on every computer and should be set to update automatically at least every week if not daily.

Appendix 3

Understanding Images

Purpose of Guide

This guide is designed to raise awareness of how digital images work and how they can be modified to work efficiently and more safely on school websites. This guidance is for all users of learning platforms and websites including pupils. It will also support the efficient use of images in word processed documents, desktop publishing and presentations.

Background

Digital images can be acquired from a number of different sources including digital cameras, scanners, art packages and the internet. They come in a number of different formats, determined by their file suffixes such as *.bmp or *.jpg.

The BMP format is a common format created by art packages such as Windows paint. Files in this format are in a raw format and are generally quite large. They are good for printing but can not be used on the internet.

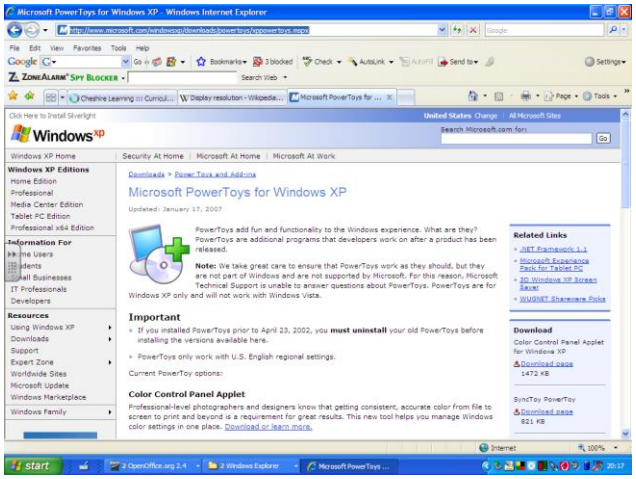
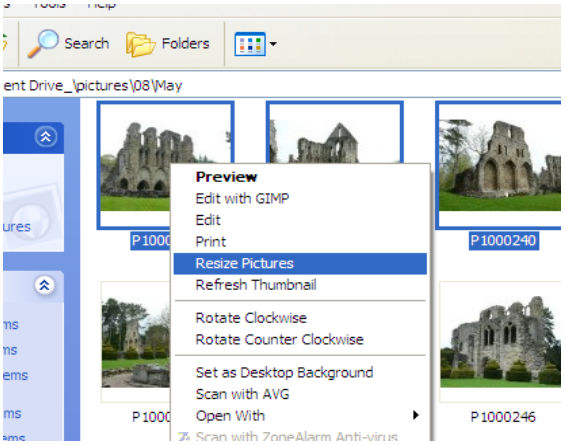
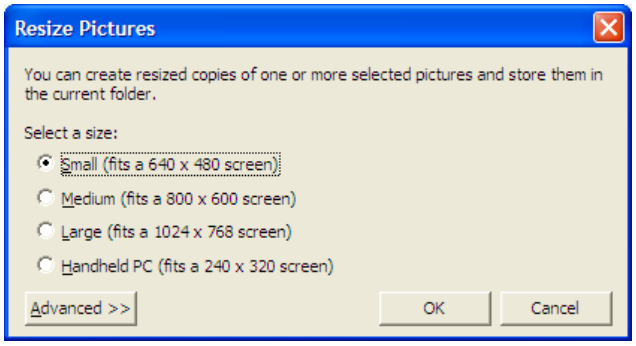
The JPG format is commonly used by digital cameras and is compatible with the internet and the vast majority of applications. This is a compressed format and when files are saved in this format they will lose some of their quality. How determinable this loss is will depend on what you are using the images for. In general it will probably not affect you. Most digital cameras use JPG as their default setting.

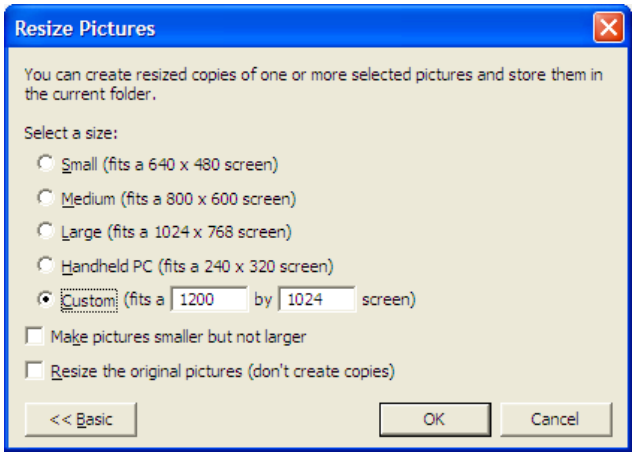
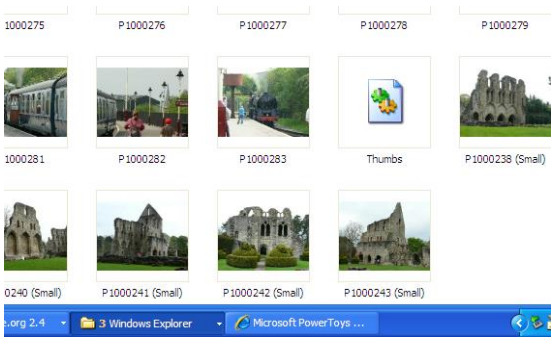
There are other image types for different uses such as GIF, PNG and the proprietary formats used by graphics packages such as Photo Shop and Gimp. Different applications are able to read and use different file formats. The internet uses very few, jpg, png and gif being the most common.

Computer screens use a variety of different resolutions and an understanding of these will help you determine the quality of the image you need to use.

Perhaps the most concerning element is that images which are uploaded to the internet in their raw state, running to many mega pixels, can be easily downloaded and manipulated by the users of the website. This is easily done by right clicking on an image on the web and choosing Save Picture As.

The simple rule then is before uploading a digital image into a document or onto a website reduce it's size and resolution to the maximum needed to serve it's purpose. This will both help with performance.

Download free of charge Image Resizer from Microsoft PowerToys at http://www.microsoft.com/windowsxp/downloads/powertoys/xppowertoys.mspx. Install it on your system.	
Once installed find a folder with images in. You can highlight individual ones or multiple images. Once highlighted right click on them and select Resize Pictures from the menu bar.	
A menu comes up. All these will reduce the size of the file, and therefore the quality. A copy of the file will be created. You need to decide how big an image you need. Generally for a web page you are unlikely to need one that is bigger than the small one, and more likely you would need a smaller one still. You can tailor these in the advanced tab and selecting custom.	

Unless you select the Resize the original pictures copies will be created in the same folder.	
The pictures will be named with the same name and (small, medium, large or custom) in brackets. These images have been reduced in size from 3.7mb to 56k. This means that they will load much quicker on the web or keep the Powerpoint or word documents small in size. The user however will not see any noticeable difference in quality on the screen or even in an A4 print out of the document.	

Recommendation

Teach all users and students how to manipulate images to reduce file size. Install software on all systems to make it simple to manipulate images.

Appendix 4

Guidance in response to an incident of concern

Internet technologies and electronic communications provide children and young people with the opportunity to broaden their learning experience and develop creativity in and out of school. However, it is also important to consider the risks associated with how these technologies are used.

Any e-Safety Policy should also recognise and seek to develop the skills that children and young people need when communicating and using these technologies properly, while keeping safe and secure, and acting with respect for other users.

These risks to e-safety are, of course, caused by people acting inappropriately or even illegally. Any potential issue must be dealt with at a personal level. Teachers are the first line of defence; their observation of behaviour is essential in detecting danger to pupils and in developing trust so that issues are reported. Incidents will vary from the prank or unconsidered action to occasional extremely concerning incidents that may involve Child Protection Officers or the Police.

This section will help staff determine what action they can take within the school and when to hand the issue over to the school-based Child Protection Co-ordinator, the e-Safety Officer or the Police Liaison Officer.

What does electronic communication include?

- **Internet collaboration tools:** social networking sites and blogs
- **Internet Research**: web sites, search engines and Web browsers
- **Mobile Phones and personal digital assistants** (PDAs)
- **Internet communications:** e-Mail and instant messaging (IM)
- **Webcams and videoconferencing**

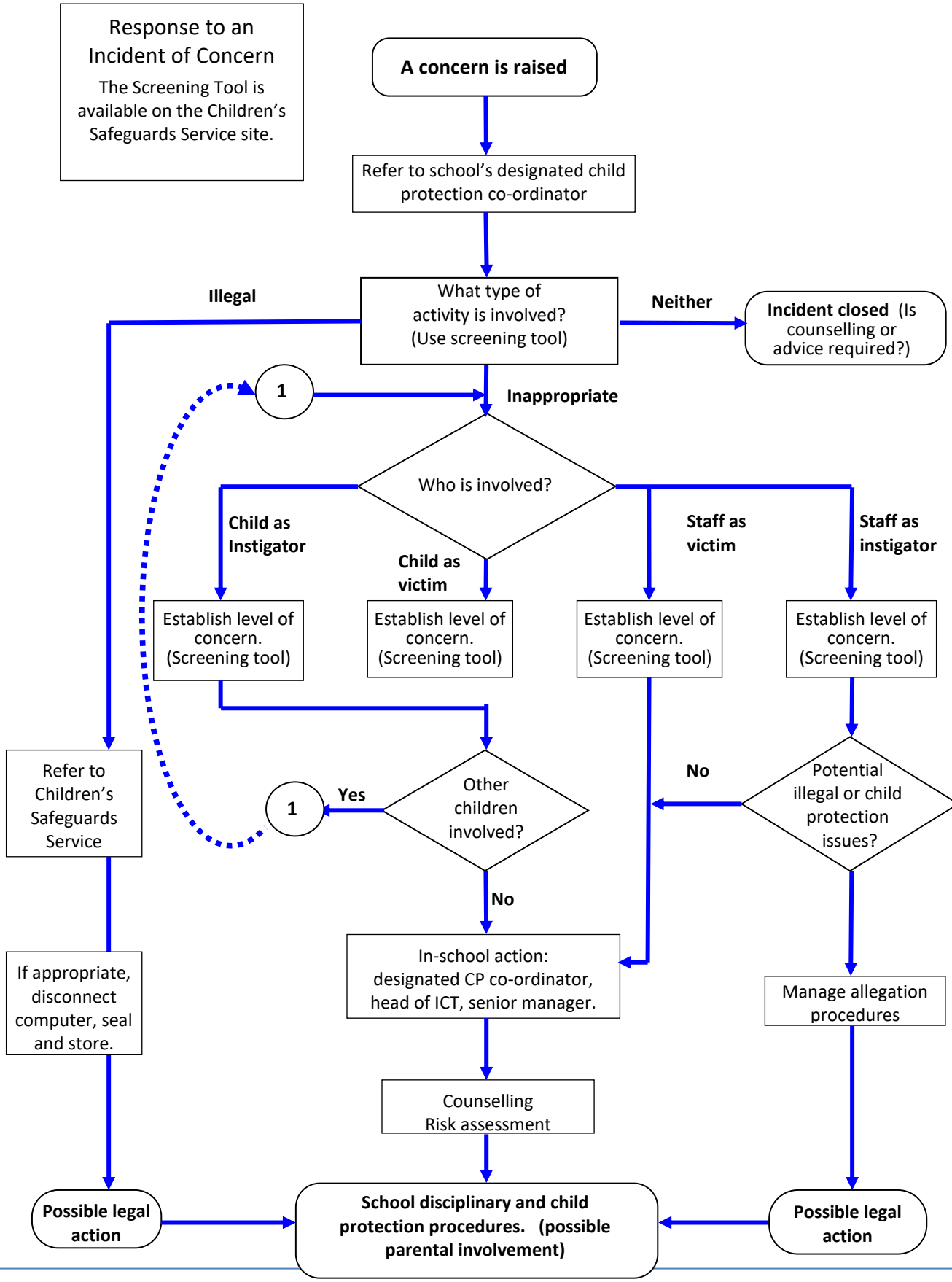
What are the risks?

- Receiving inappropriate content
- Predation and grooming
- Requests for personal information
- Viewing 'incitement' sites
- Bullying and threats
- Identity theft
- Publishing inappropriate content
- Online gambling
- Misuse of computer systems
- Publishing personal information/images
- Hacking and security breaches

How do we respond?

The flowchart on the next page illustrates the approach to investigating an incident of concern. This diagram should not be used in isolation and the Child Protection Unit and Designated staff member should be consulted.

As previously stated schools should ensure that relevant policies (Acceptable Use Policy, Behaviour Policy, Bullying Policy, Discipline Policy) are referenced and are considered when dealing with the issues identified.


Response to an Incident of Concern
The Screening Tool is available on the Children's Safeguards Service site.
A concern is raised
Refer to school's designated child protection co-ordinator
What type of activity is involved? (Use screening tool)
Illegal
Neither
Incident closed (Is counselling or advice required?)
1
Inappropriate
Who is involved?
Child as Instigator
Child as victim
Staff as victim
Staff as instigator
Establish level of concern. (Screening tool)
Establish level of concern. (Screening tool)
Establish level of concern. (Screening tool)
Establish level of concern. (Screening tool)
Refer to Children's Safeguards Service
1
Yes
Other children involved?
No
Potential illegal or child protection issues?
No
If appropriate, disconnect computer, seal and store.
In-school action: designated CP co-ordinator, head of ICT, senior manager.
Manage allegation procedures
Counselling
Risk assessment
Possible legal action
School disciplinary and child protection procedures. (possible parental involvement)
Possible legal action

Appendix 5

The following matrix offers for consideration examples of typical incidents and their respective responses:

Child as Victim				
Hazard	**Examples**	**Prevention**	**Proposed Response**	**Comments**
Receiving unsolicited content that is inappropriate, obscene, offensive or threatening	Web sites (often through mis-clicked or mis-typed web addresses); email (Spam); banner advertising; pop-ups (largely eradicated through better browser design).	Educator vigilance; Acceptable Internet Use Policy known by all users, and is enforced by school. Effective web filtering in place. Consider using safe filtered email. Effective spam filtering. Maintain email and URL logs and history.	Refer to screening tool to help determine severity of impact on the child. As the content is unsolicited, there can be no question of culpability of the child. Follow-up to prevent recurrence, including ensuring that relevant sites are blocked if required. Inform parents where appropriate. Ensure incidents are reported and recorded.	*All secondary children should have access to the Internet and personal email as an entitlement.* *Protective measures are essential; however it is not acceptable to be so risk averse that access is removed entirely. There should be procedures agreed with parents and Governors for reporting abuse.*
Publishing.	Images stored in publicly accessible areas; Personal blogs such as Details left on web sites. Incitement: hatred and discrimination, personal harm etc.	Educator vigilance; Acceptable Internet Use Policy known by all users, and children made aware of the dangers. In-house education sessions.	Refer to the screening tool to help determine the severity of impact on the child. Determine if a perpetrator / victim relationship may exist. Where an in-school perpetrator is identified, take appropriate disciplinary or legal action. Where an external perpetrator is identified, report to police or other agency. Advice should be sought from the area children's officer for child protection. Follow-up to prevent recurrence, including ensuring that relevant sites are blocked if required. Inform parents where appropriate.	*Most image storage sites have levels of access, usually private; family & friends and public. These sites are great fun for sharing images; however care should be taken as they may provide access to inappropriate public images.* *Children need to be made aware of the dangers associated with posting personal images and information on the internet.*

Bullying and threats.	email; text messaging; blogs; Instant Messaging (due to changes in the software, the perpetrator is usually known to the victim). Incitement: hatred and discrimination, personal harm etc.	Reinforcement of school ethos and behaviour. Regular sample trawls of known sites. This should be linked to the curriculum (PSHE) and Every Child matters.	Refer to the screening tool to help determine the severity of impact on the child. Determine if a perpetrator / victim relationship exists. Where a perpetrator is identified take appropriate disciplinary / legal action. Follow-up to prevent recurrence, including ensuring that relevant sites are blocked if required. Inform parents where appropriate.	*There is no real difference between bullying and threats using technology and more familiar means. Bullying and threatening behaviour is damaging and wrong and should be treated very seriously. Racist bullying could be considered an offence under the race relations act and legal consultation may be necessary.*
Predation and grooming	Forming online relationships by deception with the intent of gaining the confidence of a minor to do harm. (N.B. If you are over 18 and make contact with somebody under 16 on 2 occasions by any means inc. internet, email etc and plan to meet them anywhere in the world with a view to committing a sexual offence that is the offence of Grooming. – 2003 sexual offences act)	Teach awareness of dangers. Use the 'Think U Know' teaching resources. Liaise with Area children's officer for child protection for additional advice / training	Refer to the screening tool to help determine the severity of impact on the child. Determine if a perpetrator / victim relationship exists. Where a perpetrator is identified take appropriate disciplinary / legal action. Follow-up to prevent recurrence, including ensuring that relevant sites are blocked if required. Inform parents and police, and report to CEOP report abuse web site..	*Grooming and predation is a child protection issue and should be reported to the DCPC and the police in all cases, or referred to CEOP through their reporting web site.*
Online Gambling	Banner adverts / pop ups offering free credit for gambling.	Teach awareness of dangers to all staff and pupils. Encourage self-reporting	Inform parents. Its a criminal offence to use someone else's credit card (fraud) may need to involve the police if card owner wants to press charges. Provide help and support for child, because gambling is an addiction.	*Many children have access to their parents credit card for legitimate use e.g. online purchases, however this can be misused to enable them to access gambling sites.*
Requests for personal information.	phishing' is the use of deceit to obtain personal (usually financial) information.	Teach awareness of dangers to all staff and pupils.	If identity theft occurs it should be reported to police without exception.	*Most 'phishing' is aimed at adults with banking facilities, so older children are more likely to be affected.*

Security	Adware; browser hijack; virus.	Secure and up to date browser settings and anti-virus software; regular adware scans. Teach awareness of dangers to all staff and pupils.	Effective reactive technical intervention.	
Child as Instigator				
Hazard	**Examples**	**Prevention**	**Proposed Response**	**Comments**
Soliciting content that is inappropriate, obscene, or offensive.	Use of inappropriate search terms; Accessing or forwarding the details of known sites; Following inappropriate links or banners; inappropriate Image searches.	Use safe image search engines. Effective web filtering. Educator vigilance. Effective incident reporting procedures for blocking sites once known.	Refer to the screening tool to help determine the severity of impact on the child. Inform parents (consider standard letter templates). Restrict computer or Internet access for a fixed period, dependent on severity. Maintain incident records to identity patterns of behaviour. Follow-up to prevent recurrence, including ensuring that relevant sites are blocked if required. Inform parents where appropriate. Ensure incidents are reported and recorded.	*Maintain records of incidents to identify serial offenders.*
Viewing 'incitement' sites	Sites involving pro-anorexia, self harm, race hate, suicide, terrorism etc	Educating children of the danger of these sites. Effective web filtering to block these sites	Refer to the screening tool to help determine the severity of impact on the child. Seek advice from appropriate professionals (child protection or health) Provide a directory of sites that provide professional advice on these issues.	
Sends or publishes content that is inappropriate, obscene, offensive or threatening.	emails blogs; msn-spaces; social sites (BEBO etc.) chat rooms.	Block access to specific sites. Educate children in safe and appropriate internet use.	Refer to the screening tool to help determine the severity of impact on the child and whether an offence has taken place. Maintain records of incidents to identify serial offenders. Inform parents. (Consider standard letters). Remove computer access for a fixed period. Use school disciplinary procedure as appropriate	*Sending threatening or illegal content is an offence; refer to the glossary for more details.* *The medium is less important than intent. Publishing is easy using the web; however in legal terms it can still be libellous and subject to the same legal remedies. Where there are known sites that do not moderate effectively they should be blocked.*

			Follow-up to prevent recurrence, including ensuring that relevant sites are blocked if required. Inform parents where appropriate. Ensure incidents are reported and recorded	*Children should be made aware that publishing personal information could place themselves or others in a dangerous situation.*
Identity Theft	Using others identity to gain access to school systems or services.	Systematic changes of password. Alternative methods of authentication, such as swipe card or fingerprint.	Recover identity and change password. Inform parents (consider standard letter templates). Restrict computer or Internet access for a fixed period, dependent on severity.	*This is a potential criminal activity and advice should be sought from the Police.* *It is essential that schools consider carefully where personal data is stored, and by whom they can be accessed. This will become increasingly important as data starts to be warehoused off-site. Access to names and addresses must be secure, and CRB checks in place to protect children.*
Interception of communications	Diverting email; wireless interception.	Effective network security.	Change encryption keys and/or passwords, or delete and rename email addresses. Consider whether the interception has led others to be placed at risk.	*This can be the interception of wireless communications, or even attempting to access a wireless network without permission. There is an implicit expectation that security measures are in place.*
Hacking	Purposeful intrusion or damaging of network services.	High level of security on administrator passwords; restricted issue; do not leave open administrator accounts open when not in use; Rehearse back-up and recovery procedures.	Restore from back-up. Consider whether the hacking has caused others to be placed at risk e.g. the instigator putting illegal content onto other users computers.	*Most hacking in schools is from highly able individuals who are attracted by the technical challenge. It is often better to harness the skills and enthusiasm through constructive activities in support of the network management.* *The exception is where it is purposefully belligerent in nature, or targeted on individuals or their work.*

Appendix 6

Screening Tool

This screening tool can be used to assist decision making in dealing with incidents of computer or e-communications misuse within your school. It can be used to inform initial action but is not a substitute for a thorough risk assessment/investigation.

This should be used alongside the e-Safety flow chart and incidents of misuse matrix.

If you are concerned that a child may have been a victim of a criminal offence or suffered child abuse, please contact a member of the Child Protection Unit.

Type of incident

Sexual	[ ]
Bullying	[ ]
Violence	[ ]
Incitement	[ ]
Financial	[ ]
Grooming	[ ]
Other	[ ]

How was the incident discovered?

Self-reported	[ ]
Reported by 3rd party (friends or parents)	[ ]
Reported by Teacher	[ ]
Other (e.g. Police, Social Services, etc)	[ ]

What was their response to the incident?

Unconcerned	[ ]
Curious	[ ]
Distressed	[ ]
Frightened	[ ]
Secretive	[ ]
Other	[ ]

What did the incident refer to?
Answer the key questions relating to the particular incident

Child as Victim:

Content

1. What was the type of content? (Sexual, violence, racial, other) ……
2. Did anyone else see it? [ ] ……..
3. Have they told anyone else about it? [ ] ……..

Publishing

1. Is the child identifiable? [ ]
2. Can their location be traced? [ ]
3. Is text or image potentially indecent or illegal? [ ]

Bullying

1. What was the type of bullying? (sexual, violent, physical, group) …….
2. Was information or images published of the child? [ ]
   (If yes, refer back to publishing section for more questions to ask)

Predation / Grooming

1. Assess the extent of the contact
   - One off conversation [ ]
   - Regular conversation [ ]
   - Regular conversation using inappropriate or sexualised language or threats [ ]
   - Attempts to breakaway [ ]
   - Offline meeting arranged [ ]
   - Offline meeting occurred [ ]
   - (Consider if an offence has occurred)
2. Are the parents aware? [ ]
3. When did the incident occur? ……

Request for information

1. Did the child give out any personal information? [ ]

<u>Child as Victim</u>:

Content

Refer to 'Child as Victim' questions on content
Refer to the matrix to assess the child's response to the content

Incitement

1. Was the child secretive about the site? [ ]
2. Did the child access the site in an isolated place? [ ]
3. Did they understand the risks of accessing this site? [ ]
4. What was their response to the site?
   - Healthy (e.g. using for research) [ ]
   - Problematic (looking for advice or guidance) [ ]
   - Harmful [ ]
   - (relying on site for tips, using site to communicate with likeminded individuals, the site is reinforcing /minimising potentially harmful behaviours e.g. self-harm, pro anorexia sites)

Send/Publishing

1. Has an offence taken place? [ ]
   (refer to glossary for information on what constitutes an offence)
2. Were others put at risk e.g. their image / information was sent / published? [ ]
3. Was this an isolated incident or persistent? [ ]
4. Did the instigator have empathy for the victim? [ ]

Interception of communications / Hacking

1. Have they placed themselves or others at risk? [ ]
2. Has personal or financial information been stolen? [ ]

(if yes, this constitutes a criminal offence and advice should be sought from the police)

3. Has illegal content been accessed and sent to other's computers? [ ]

Once you have gathered the appropriate information, assess the effect of the incident on the child and identify how the child can be best supported. This may be either in school (using existing policies and resources to support children) or in certain circumstances with external help.

Staff misuse

1. Did the member of staff misuse the school's internal email system? [ ]

2. Did the member of staff communicate with a young person inappropriately [ ]
3. e.g. via text message, multimedia images.

4. Consider the extent of the communication

One off conversation	[ ]
Regular conversation	[ ]
Regular conversation using inappropriate or sexualised language or threats	[ ]
Attempts to breakaway	[ ]
Offline meeting arranged	[ ]
Offline meeting occurred	[ ]
(Consider if an offence has occurred)	

5. Did the member of staff access inappropriate/ illegal material within school? [ ]

6. Did the member of staff access inappropriate/ illegal material using school equipment? [ ]

7. Did the member of staff access inappropriate/ illegal material using their own equipment? [ ]

If you are concerned that a child may have been a victim of a criminal offence or suffered child abuse, please contact a member of the Child Protection Unit before taking any other action.

Appendix 7

E safety Audit

This quick self-audit will help the senior management team (SMT) assess whether the E safety basics are in place. Has the school an E-safety Policy that complies with CYPD guidance?

Has the school an E-safety Policy?	Yes
Date of latest update:	2019
The Policy was agreed by governors on:	21st May 2019
The Policy is available for staff at:	Staff handbook, office and Staffshare School website Policy folder, office Safeguarding folder, office
And for parents at:	School website
The designated Child Protection Teacher/Officer is	Helen Kelly Gemma Williams & Sam Orton (Deputies)
The E-safety Coordinator is:	Helen Kelly
The E safety Governor is:	Paul Corbishley
Has E-safety training been provided for both pupils and staff?	Yes, annually
Do all staff sign an ICT Code of Conduct on appointment?	Yes
Do children sign an agreement about responsible IT use?	Yes, Years 3-6
Are parents sent a copy of the Acceptable Use Agreement for KS2 pupils?	Available on school website
Have school E safety rules been set for pupils?	Yes, in Acceptable Use Agreement
Are these rules displayed in all rooms with computers?	Yes
Internet access is provided by an approved educational Internet service provider and complies with DFE requirements for safe and secure access	Yes, internet provided by Cheshire West and Chester
Is personal data collected, stored and used according to the principles of the Data Protection Act 2018?	Yes
Is a log kept of any data breaches	Yes, as required
Is there communication between the E-Safety Co-ordinator and the E-Safety Governor	Yes

Glossary

Many young people use the internet regularly without being aware that some of the activities they take part in using the internet are potentially illegal.

The 2003 Sexual offences Act has introduced new offences of Grooming and raised the age for making/distributing indecent images of children to 18.

Offences regarding racial hatred are covered by the Public Order Act 1986 although there is currently a new Racial and Religious Hatred Bill going through parliament.

Bullying etc could be an offence under the Malicious Communications Act 1988 or Telecommunication Act 1984

Other potential offences may include Fraud (e.g. using false identities) or infringements of the General Data Protection Act 2018.

List of offences:

Sexual Offences Act 2003
Grooming – If you are over 18 and have communicated with a child under 16 at least twice (including by phone or 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.

Making indecent images – it is an offence to take, make, distribute, show, advertise indecent images of a child under 18.
(NB to view an indecent image on your computer means that you have made a digital image.)

Causing a child under 16 to watch a Sexual Act – to intentionally cause a child to watch someone else taking part in sexual activity, including looking at images such as videos, photos or webcams, for your own gratification.

Abuse of positions of trust. Staff need to be aware that it is 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. (applies to teachers, social workers, health professionals, connexions Pas)

N.B. Schools should already have a copy of 'Children & Families: Safer from Sexual Crime' document as part of their child protection packs.
Alternatively information about the 2003 Sexual Offences Act can be found at www.teachernet.gov.uk

Public Order Act 1986 – offence to possess, publish, disseminate material intended to/likely to incite racial hatred.

Telecommunications Act 1984 – Offence to send by public telecommunications network any offensive, indecent, obscene or menacing messages that cause annoyance/inconvenience/needless anxiety.

Malicious Communications Act 1988 – offence to send letter or article which includes indecent, grossly offensive, threatening or false information with the intent of causing anxiety/stress to the recipient.

Protection from Harassment Act 1997 –
Section 1 - 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.
Section 4 - 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.

General Data Protection Act 2018
The Principles:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');

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

Article 5(2) adds that:
The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').