Discovering the best in everyone

DIOCESE OF WORCESTER
MULTI ACADEMY TRUST
TO LOVE | TO LEARN | TO SERVE

ST. NICHOLAS
C of E MIDDLE SCHOOL

FEDERATION OF ST. NICHOLAS C OF E MIDDLE SCHOOL, PINVIN, AND PINVIN C OF E FIRST SCHOOL

E Safety Policy

Created on	Feb 2021
Frequency	Annually
Date of next review	January 2022

Agreed by …………………………………. ………………………………………….
(Headteacher) (Chair of Governors)

Date Agreed …………………….............

School Details

E-safety Governor: Richard Elliott

E-safety Co-ordinator: Mr Martin Davids

Headteacher: Mrs S Jennings

Ratified by Governing Body on: Feb 2021

Next review date: January 2022

Background and rationale

The potential that technology has to impact on the lives of all citizens increases year on year. This is probably even more true for children, who are generally much more open to developing technologies than many adults. In many areas, technology is transforming the way that schools teach and that children learn. At home, technology is changing the way children live and the activities in which they choose to partake; these trends are set to continue.

While developing technology brings many opportunities, it also brings risks and potential dangers of which these are just a few:

- Access to illegal, harmful or inappropriate images or other content
- Allowing or seeking unauthorised access to personal information
- Allowing or seeking unauthorised access to private data, including financial data
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual’s consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive or addictive use which may impact on social and emotional development and learning.

This policy sets out how we strive to keep children safe with technology while they are in school. We recognise that children are often more at risk when using technology at home (where we have no control over the technical structures put in place to keep them safe) and so this policy also sets out how we educate children about the potential risks. We also explain how we attempt to inform those people who work with our children beyond the school environment (parents, friends and the wider community) to be aware and to assist in this process.

Our school’s e-safeguarding policy has been written from a template provided by Worcestershire School Improvement team which has itself been derived from that provided by the South West Grid for Learning.

A. Policy and leadership

This section begins with an outline of the **key people responsible** for developing our E-Safety Policy and keeping everyone safe with ICT. It also outlines the core responsibilities of all users of ICT in our school.
It goes on to explain **how we maintain our policy** and then to outline **how we try to remain safe while using different aspects of ICT**

A.1.1 Responsibilities: e-safety coordinator

Our e-safety coordinator is the person responsible to the head teacher and governors for the day to day issues relating to e-safety. The e-safety coordinator:

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school ICT technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments as soon as they occur
- reviews weekly the output from monitoring software and initiates action where necessary
- meets regularly with the e-safety governor to discuss current issues and review incident logs
- reports current issues to the Headteacher.
- receives appropriate training and support to fulfil their role effectively

A.1.2 Responsibilities: governors

Governors are responsible for the approval of this policy and for reviewing its effectiveness. This will be carried out by the governors (or a governors' subcommittee) receiving regular information about e-safety incidents and monitoring reports. A member of the governing body has taken on the role of e-safety governor which involves:

- regular meetings with the E-Safety Co-ordinator annually with an agenda based on:
  - monitoring of e-safety incident logs
  - reporting to relevant Governors committee / meeting

A.1.3 Responsibilities: head teacher

- The head teacher is responsible for ensuring the safety (including e-safety) of all members of the school community, though the day to day responsibility for e-safety is delegated to the E-Safety Co-ordinator
- The head teacher will be familiar with the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff, including non-teaching staff. (see flow chart on dealing with e-safety incidents (included in section 2.6 below) and other relevant Local Authority HR / disciplinary procedures)

A.1.4 Responsibilities: classroom based staff

Teaching and Support Staff are responsible for ensuring that:

- they safeguard the welfare of children and refer child protection concerns using the proper channels: **this duty is on the individual, not the organisation or the school**.

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school’s Acceptable Use Agreement for staff
- they report any suspected misuse or problem to the E-Safety Co-ordinator
- they undertake any digital communications with pupils (email) in a fully professional manner and only using official school systems (see A.3.5)
- they embed e-safety issues in the curriculum and other school activities, also acknowledging the planned e-safety programme (see section C)

A.1.5 Responsibilities: ICT technician

The ICT Technician is responsible for ensuring that:

- the school’s ICT infrastructure and data are secure and not open to misuse or malicious attack
- the school meets the e-safety technical requirements outlined in section B.2.2 of this policy (and any relevant Local Authority E-Safety Policy and guidance)
- users may only access the school’s networks through a properly enforced password protection policy as outlined in the school's e-security policy
- shortcomings in the infrastructure are reported to the ICT coordinator or head teacher so that appropriate action may be taken.

A.2.1 Policy development, monitoring and review

This e-safety policy has been developed (from a template provided by Worcestershire School Improvement Service) by a working group made up of:

- School E-Safety Coordinator
- Head teacher
- Teachers
- Governors *(*especially the e-safety governor*)*
- Pupils

A.2.2 Policy Scope

This policy applies to **all members of the school community** (including teaching staff, wider workforce, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, **both in and out of school**.

The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but are linked to membership of the school.

The school will deal with such incidents using guidance within this policy as well as associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

A.2.3 Acceptable Use Agreements

All members of the school community are responsible for using the school ICT systems in accordance with the appropriate acceptable use policy, which they will be expected to sign before being given access to school systems.

Acceptable Use Agreements are provided in Appendix 2 of this policy for:

- Pupils (EYFS + KS1 / KS2)
- Staff (and volunteers)
- Parents / carers
- Community users of the school's ICT system

Acceptable Use Agreements are introduced at parents' induction meetings and signed by all children as they enter school (with parents signing on behalf of children in Reception). Children re-sign when entering a new class.

All employees of the school and volunteers sign when they take up their role in school and in the future if significant changes are made to the policy.

Parents sign once when their child enters the school. The parents' policy also includes permission for use of their child's image (still or moving) by the school, permission for their child to use the school's ICT resources (including the internet) and permission to publish their work.

Community users sign when they first request access to the school's ICT system.

A.2.4 Self Evaluation

Evaluation of e-safety is an ongoing process and links to other self evaluation tools used in school in particular to pre-Ofsted evaluations along the lines of the Self Evaluation Form (SEF). The views and opinions of all stakeholders (pupils, parent, teachers …) are taken into account as a part of this process.

A.2.5 Whole School approach and links to other policies

This policy has strong links to other school policies as follows:

Anti-bullying	How your school strives to eliminate bullying – link to cyber bullying
Safeguarding and Child Protection	Safeguarding children electronically is an important aspect of E-Safety*. **The e-safety policy forms a part of the school's safeguarding policy***
Behaviour	Positive strategies for encouraging e-safety and sanctions for disregarding it.

A.2.6 Illegal or inappropriate activities and related sanctions

The school believes that the activities listed below are inappropriate in a school context **(those in bold are illegal)** and that users should not engage in these activities when using school equipment or systems (**in or out of school**).
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on material, remarks, proposals or comments that contain or relate to:

- **child sexual abuse images (illegal - The Protection of Children Act 1978)**
- **grooming, incitement, arrangement or facilitation of sexual acts against children (illegal – Sexual Offences Act 2003)**
- **possession of extreme pornographic images (illegal – Criminal Justice and Immigration Act 2008)**

- **criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation or gender identity) (illegal – Public Order Act 1986)**
- pornography
- promotion of any kind of discrimination
- promotion of racial or religious hatred
- threatening behaviour, including promotion of physical violence or mental harm
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute

Additionally the following activities are also considered unacceptable on ICT equipment or infrastructure provided by the school:

- Using school systems to undertake transactions pertaining to a private business
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Worcestershire County Council Broadband and / or the school
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files that causes network congestion and hinders others in their use of the internet)
- On-line gambling and non educational gaming
- Personal on-line shopping / commerce
- Use of social networking sites (other than in the school's learning platform or sites otherwise permitted by the school)

If members of staff suspect that misuse might have taken place – whether or not it is evidently illegal (see above) - it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. Please see **Appendix 3.**

It is more likely that the school 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 / disciplinary procedures.

A.2.7 Reporting of e-safety breaches

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

- Particular care should be taken if any apparent or actual misuse appears to involve illegal activity listed in section A.2.6 of this policy.
- If in any doubt, talk to the e-safety co-ordinator, head teacher or e-safety governor.

A.3.1 Use of hand held technology (personal phones and hand held devices)

We recognise that the area of mobile technology is rapidly advancing and it is our school's policy to review its stance on such technology on a regular basis. Currently our policy is this:

- Members of staff (Early Years) are not permitted to bring their personal mobile device into the setting, and are not allowed to use it at any point when any child is present.
- Members of staff (KS1 and KS2) are permitted to bring their personal mobile devices into school. They are required to use their own professional judgement as to when it is appropriate to use them. Broadly speaking this is:
    - ✓ Personal hand held devices will be used in lesson time only in an emergency or extreme circumstances
    - ✓ Members of staff are free to use these devices outside teaching time.
    - ✓ Members of staff must leave these devices in a bag away from their person. They will be allowed to have them in a pocket in emergency circumstances.
- Pupils are not currently permitted to bring their personal hand held devices into school.

A.3.2 Use of communication technologies

A.3.2a - Email

Access to email is provided for all users in school via the DOWMAT email system. In addition, these official school email services may be regarded as safe and secure and are monitored.

- Staff and pupils should primarily use the school email services to transfer information with others when in school, or on school systems (e.g. by remote access)
- Pupils only use a class email account to communicate with people inside and outside of school and with the permission / guidance of their class teacher. When communicating with people outside of school, the contacts are approved by the teacher.
- A structured education program is delivered to pupils which helps them to be aware of the dangers of, and good practices associated with, the use of email (see section C of this policy)
- Staff may access their personal e-mail accounts during school hours for purpose of school business or in an emergency.
- Users need to be aware that email communications may be monitored
- Users must immediately report to their class teacher / e-safety coordinator – in accordance with the school policy (see sections A.2.6 and A.2.7 of this policy) - the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and they must not respond to any such email.

A.3.2b - Social networking (including chat, instant messaging, blogging etc)

	Staff / adults				Pupils			
Use of social networking tools *It is important that schools review this table in the light of principles agreed within their own establishment.*	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff	Not allowed
Use of non educational chat rooms etc				✓				✓
Use of non educational instant messaging				✓				✓
Use of non educational social networking sites				✓				✓
Use of non educational blogs				✓				✓

A.3.2c – Videoconferencing / Skype

Desktop video conferencing and messaging systems linked to WCC Broadband via MS Communicator is the preferred communication option in order to secure a quality of service that meets school curriculum standards.

Videoconferencing equipment in classrooms must be switched off when not in use and not set to auto answer. If using Skype app on IPads, app will only be opened under adult supervision.

External IP addresses should not be made available to other sites.

Only web based conferencing products that are authorised by the school (and are not blocked by internet filtering) are permitted for classroom use.

Videoconferencing is normally supervised directly by a teacher. In the event of this not being the case pupils must ask permission from the class teacher before making or answering a videoconference call.

Permission for children to take part in video conferences is sought from parents / carers at the beginning of the pupil's time in school (see section A.2.3 and Appendix 2). Only where permission is granted may children participate.

Only key administrators have access to videoconferencing administration areas.

Unique log on and password details for the educational videoconferencing services (such as the Janet booking system) are only issued to members of staff.

A.3.3 Use of digital and video images

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. (See section C). In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Members of staff are allowed to take digital still and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. These images must be taken on school equipment, not personal equipment. The equipment must be left at school at the end of the school day/visit.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

- Pupils must not take, use, share, publish or distribute images of others without their permission

Also see the following section (A.3.4) for guidance on publication of photographs

A.3.4 - Website (and other public facing communications)

Our school uses the public facing website (http://www.crowle.worcs.sch.uk/) only for sharing information with the community beyond our school. This includes, from time-to-time, celebrating work and achievements of children. All users are required to consider good practice when publishing content.

- Personal information will not be posted on the school website and only official email addresses will be used to identify members of staff (never pupils).
- Only pupil's first names will be used on the website, and only then when necessary.
- Detailed calendars will not be published on the school website.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with the following good practice guidance on the use of such images:
  - ✓ pupils' full names will not be used anywhere on a website or blog, and never in association with photographs
  - ✓ where possible, photographs will not allow individuals to be recognised
  - ✓ written permission from parents or carers will be obtained before photographs of pupils are published on the school website (see section A.2.3 and Appendix 2)
- Pupil's work can only be published with the permission of the pupil and parents or carers. (see section A.2.3 and Appendix 2)

:

A.3.5 - Professional standards for staff communication

In all aspects of their work in our school, teachers abide by the **Teachers' Standards** as described by the DfE effective from September 2012: http://media.education.gov.uk/assets/files/pdf/t/teachers%20standards.pdf.
Teachers translate these standards appropriately for all matters relating to e-safety.

Any digital communication between staff and pupils or parents / carers (email, chat, etc) must be professional in tone and content.

- These communications may only take place on official (monitored) school systems.
- Personal email addresses, text messaging or public chat / social networking technology must not be used for these communications.

Staff constantly monitor and evaluate developing technologies, balancing risks and benefits, and consider how appropriate these are for learning and teaching. These evaluations help inform policy and develop practice.
The views and experiences of pupils are used to inform this process also.

B. Infrastructure

B.1 Password security

This is dealt with in detail in our school's **E-security Procedures** (see appendix 1). Please refer to that document for more information.

The school's e-safety curriculum will include frequent discussion of issues relating to password security and staying safe in and out of school (see section C of this policy)

B.2.1 Filtering

B.2.1a - Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the school has a filtering policy, (Policy Central) to manage the associated risks and to provide preventative measures which are relevant to the situation in this school. As a school buying broadband services from Worcestershire County Council, we automatically receive the benefits of a managed filtering service, with some flexibility for changes at local level.
It is recognised that the school can take full responsibility for filtering on site but current requirements do not make this something that we intend to pursue at this moment.

B.2.1b - Responsibilities

The day-to-day responsibility for the management of the school's filtering policy is held by the **e-safety coordinator** (with ultimate responsibility resting with the **head teacher and governors**). They manage the school filtering in line with this policy and keep logs of changes to and breaches of the filtering system.

- To ensure that there is a system of checks and balances and to protect those responsible, changes to the standard Worcestershire school filtering service must be reported to a second responsible person (the head teacher / E-safety coordinator / e-safety governor) within the time frame stated in section A.1.3 of this policy

All users have a responsibility to report immediately to class teachers / e-safety coordinator any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.
Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

B.2.1c - Education / training / awareness

Pupils are made aware of the importance of filtering systems through the school's e-safety education programme (see section C of this policy).

Staff users will be made aware of the filtering systems through:

- signing the Acceptable Use Agreement (as part of their induction process)
- briefing in staff meetings, training days, memos etc. (timely and ongoing).

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement.

B.2.1d - Changes to the filtering system

Where a member of staff requires access to a website that is blocked for use at school, the process to unblock is as follows:

- The teacher makes the request to the school e-safety coordinator.
- The e-safety coordinator checks the website content to ensure that it is appropriate for use in school.
- If agreement is reached, the e-safety coordinator makes a request to the Broadband Team
- The Broadband helpdesk will endeavour to unblock the site within 24 hours. This process can still take a number of hours so teaching staff are required to check websites in advance of teaching sessions.
- School Improvement Service Learning Technologies staff may then be notified of websites that have been unblocked to review them in partnership with the Broadband Team. If sites are found to not be appropriate, access will be discussed with the school and then removed.

The e-safety coordinator will need to apply a rigorous policy for approving / rejecting filtering requests. This can be found in Appendix 4 but the core of this should be based on the site's content:

- The site promotes equal and just representations of racial, gender, and religious issues.
- The site does not contain inappropriate content such as pornography, abuse, racial hatred and terrorism.
- The site does not link to other sites which may be harmful / unsuitable for pupils.

B.2.1e - Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment, especially IPads. Children will not be allowed to use IPads unattended.

Monitoring takes place as follows:

- The e-safety co-ordinator reviews the Policy Central console captures weekly. The 'report' is signed and dated by both the e-safety co-ordinator and another member of staff.
- "False positives" are identified and deleted.
- Potential issues are referred to an appropriate person depending on the nature of the capture.
- Teachers are encouraged to identify in advance any word or phrase likely to be picked up regularly through innocent use (e.g. 'goddess' is captured frequently when a class is researching or creating presentations on the Egyptians) so that the word can be allowed for the period of the topic being taught.

B.2.1f - Audit / reporting

Filter change-control logs and incident logs are made available to:

- the e-safety governor within the timeframe stated in section A.1.3 of this policy
- the Headteacher (see A.1.1)
- the Worcestershire Safeguarding Children Board on request

This filtering policy will be reviewed, with respect to the suitability of the current provision, in response to evidence provided by the audit logs.

B.2.2 Technical security

This is dealt with in detail in **IBS School's System and Data Security advice**. Please see that document for more information.

B.2.3 Personal data security (and transfer)

This is dealt with in detail in **IBS School's System and Data Security advice**. Please see that document for more information.

Teachers frequently discuss issues relating to data security and how it relates to staying safe in and out of school (see section C of this policy).

C. Education

C.1.1 E-safety education

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience. This is particularly important for helping children to stay safe out of school where technical support and filtering may not be available to them.

E-Safety education will be provided in the following ways:

- A planned e-safety programme is provided as part of ICT, PHSE and other lessons. This is regularly revisited, covering the use of ICT and new technologies both in school and outside school. The teaching of E-safety in spread throughout the year in all classes and is recorded on a whole school long term planning map.
- A planned e-safety day once a year to promote e-safety amongst parents and pupils, where lessons are dedicated to educating pupils about the risks regarding e-safety and how to deal with them correctly.
- We use the resources on the Worcestershire E-safety website as a source of e-safety education resources http://www.wes.networcs.net (e.g. Hector's World at KS1 and Cyber Café and SAFE social networking at KS2)
- Learning opportunities for e-safety are built into the *Knowledge and Understanding* sections of the *Worcestershire Primary ICT Progressions* where appropriate and are used by teachers to inform teaching plans.
- Key e-safety messages will be reinforced through further input via assemblies and pastoral activities, as well as informal conversations when the opportunity arises.
- Pupils will be helped to understand the need for the pupil Acceptable Use Agreement (see Appendix 2) and encouraged to adopt safe and responsible use of ICT both within and outside school. The Acceptable User Policy is displayed every time the children log in to a computer. All users have to agree to the policy, otherwise they will not be able to go any further on the computer.
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit, encouraging children to discuss anything of which they are unsure and implementing the expected sanctions and/or support as necessary.

- Pupils are made aware of what to do should they experience anything, while on the internet, or on the computers in general, which makes them feel uncomfortable.

C.1.2 Information literacy

- Pupils should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information by employing techniques such as:
  - ✓ Checking the likely validity of the URL (web address)
  - ✓ Cross checking references (Can they find the same information on other sites?)
  - ✓ Checking the pedigree of the compilers / owners of the website
  - ✓ See lesson 5 of the Cyber Café Think U Know materials below
  - ✓ Referring to other (including non-digital) sources
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils are taught how to make best use of internet search engines to arrive at the information they require
- We use the resources on CEOP's Think U Know site as a resource for our e-safety education http://www.thinkuknow.co.uk/teachers/resources/

C.1.3 The contribution of the children to e-learning strategy

It is our general school policy to encourage children to play a leading role in shaping the way our school operates and this is very much the case with our e-learning strategy. Children often use technology out of school in ways that we do not in school and members of staff are always keen to hear of children's experiences and how they feel the technology (especially rapidly developing technology such as mobile devices) could be helpful in their learning. Through annual audits, children's use of technology is analysed and results from these surveys help influence e-safety lessons, information for parents and also opportunities for technology to be used in lessons where appropriate.

C.2 Staff training

It is essential that all staff – including non-teaching staff - receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- Formal e-safety training will be made available to staff on an annual basis at the start of a new academic year (September).
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and acceptable use policies which are signed as part of their induction
- The E-safety Co-ordinator will be CEOP trained.
- The E-Safety Coordinator will receive regular updates through attendance at local authority or other training sessions and by reviewing guidance documents released by the DfE, the local authority, the WSCB and others.
- All teaching staff have been involved in the creation of this e-safety policy and are therefore aware of its content
- The E-Safety Coordinator will provide advice, guidance and training as required to individuals as required on an ongoing basis.
- External support for training, including input to parents, is sought from Worcestershire School Improvement Learning Technologies Team when appropriate

C.3 Governor training

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are involved in ICT, e-safety, health and safety or child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority (Governor Services or School Improvement Service), National Governors Association or other bodies.
- Participation in school training / information sessions for staff or parents

The e-safety governor works closely with the e-safety coordinator and reports back to the full governing body (see section A.1.3)

C.4 Parent and carer awareness raising

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. “There is a generational digital divide”. (Byron Report).

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site.
- Reference to the parents materials on the Worcestershire E-safety website (http://www.wes.networcs.net) or others (see Appendix 5)

C.5 Wider school community understanding

Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

Community Users who access school ICT systems /website as part of the Extended School provision will be expected to sign an Acceptable Use Agreement (see Appendix 2) before being provided with access to school systems.

Appendix 1 – E-safety procedures for Pinvin Federation of Schools

1. Introduction

This document defines the basic security requirements that must be met when processing, storing and handling data to ensure that data is held securely and only accessed by those authorised to do so.

It is the responsibility of all parties accessing schools' IT systems to comply with the requirements of these guidelines.

2. Data Security definition:

Data security legislation means that all those who hold personal data; whether on paper or electronically, must keep that data secure. Clearly, this also applies to schools. Personal data is defined as any combination of data items that identify an individual and provide specific information about them, their families or circumstances. This includes names, contact details, gender, date of birth, as well as other sensitive information such as academic achievements, other skills and abilities, and progress in school. It also includes behaviour and attendance records.

The biggest risk to data security is posed by how users manage the security of that data. This means YOU!

3. Passwords

All staff must ensure that sensitive information is physically secured or password protected.
In order to minimise the risk involved in accessing the IT systems users are required to adhere to the following:

- Always log out, or “lock” the screen when leaving your computer unattended
- 'Strong' passwords should be used – don’t use simple or obvious passwords use a mixture of capital letters, lower case letters and numbers.
- Never share passwords with others, never tell your password to anyone
- Never write passwords down and leave them near the computer
- Don’t use work passwords for personal online accounts
- Never use your user name as a password
- Never email your password or use it in an instant message

It is your personal responsibility to ensure your device is kept secure, in accordance with the following guidelines.

4. Data Protection

- Staff must comply with the Data Protection Act and the school’s Acceptable Use Policy at all times
- Sensitive data must never be copied to unauthorised locations/devices (eg. Personal USB Memory sticks, Home PCs, etc.) – remember that databases may contain sensitive data
- Data must be accurate, relevant and current
- Master documents need to be secure and backed up – data should never be solely stored on an external device (eg. a USB Memory stick)
- When deleting sensitive data, ensure you also empty the Recycle Bin
- Mobile devices (such as laptops, XDAs or external hard disk drives) are subject to the same security considerations as any other computer

5. Equipment Security

- IT Equipment holding sensitive data must be encrypted and locked away when not in use.
- IT Equipment issued to staff remains the responsibility of that individual at all times - they must never be ”loaned” to another individual (including family members)
- Laptops and all other mobile devices (eg. USB Memory sticks) must be kept secure at all times
- All laptops must connect to the school's network at least once each ½ term to allow for software and anti-virus updates

6. Other good practice

- Always turn off your computer using the Shut Down option – never use Standby, Sleep or Hibernate and never just close the lid (laptops)
- Beware of people watching as you enter passwords or view sensitive information
- Always store equipment securely
- Don't leave equipment unattended in an unsecure location
- Don't use public wireless hotspots

For further information please refer to the IBS Schools System and Data Security document which can be found on the IBS Schools website at ibsschools.worcestershire.gov.uk

Appendix 2 – Acceptable Use Agreement templates

2a – Acceptable use policy agreement – Pupils (KS1)

This is how we stay safe when we use computers:

- I will ask an adult if I want to use the computer or Ipad
- I will only use activities or apps if an adult says it is OK.
- I will take care of the computer, Ipad and other equipment
- I will ask for help from an adult if I am not sure what to do or if I think I have done something wrong.
- I will turn off the monitor or turn the Ipad over and tell an adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer.

I understand these computer rules and will do my best to keep them

My name:	
Signed (child):	
OR Parent's signature:	
Date:	

2b – Acceptable use policy agreement – pupil (KS2)

Technology Acceptable Use Agreement – Pupils (KS2)

I understand that while I am a member of Pinvin Federation of Schools I must use technology in a responsible way.

For my own personal safety:

- I understand that my use of technology (especially when I use the internet) will be supervised and monitored.
- I will keep my password safe and will not use anyone else's (even with their permission)
- I will keep my own personal information safe as well as that of others.
- I will tell a trusted adult if anything makes me feel uncomfortable or upset when I see it online.

For the safety of others:

- I will not interfere with the way that others use their technology.
- I will be polite and responsible when I communicate with others,
- I will not take or share images of anyone without their permission.

For the safety of the school:

- I will not try to access anything illegal.
- I will not download anything that I do not have the right to use.
- I will not deliberately bypass any systems designed to keep the school safe.
- I will tell a responsible person if I find any damage or faults with technology, however this may have happened.
- I will not attempt to install programmes of any type on the devices belonging to the school without permission.

KS2 Pupil Acceptable Use Agreement Form

I understand that I am responsible for my actions and the consequences. I have read and understood the above and agree to follow these guidelines:

Name:	
Signed:	
Date:	

2c - Acceptable Use Agreement – staff & volunteer

Technology Acceptable Use Agreement – Staff and Volunteers

Whilst our school promotes the use of technology, and understands the positive effects it can have on enhancing pupils' learning and community engagement, we must also ensure that staff use technology appropriately. Any misuse of technology will not be taken lightly, and will be reported to the Headteacher in order for any necessary further action to be taken.

This acceptable use agreement is designed to outline staff responsibilities when using technology, whether this is via personal devices or school devices, or on/off the school premises, and applies to all staff, volunteers, contractors and visitors.

Please read this document carefully, and sign below to show you agree to the terms outlined.

1. **Using technology in school**

- I will only use ICT systems, such as computers (including laptops) and tablets, which have been permitted for my use by the Headteacher.
- I will only use the approved email accounts that have been provided to me.
- I will not use personal emails to send and receive personal data or information.
- I will not share sensitive personal data with any other pupils, staff or third parties.
- I will ensure that any personal data is stored in line with GDPR.
- I will delete any chain letters, spam and other emails from unknown sources without opening them.
- I will ensure that I obtain permission prior to accessing learning materials from unapproved sources.
- I will only use the internet for personal use during out-of-school hours, including break and lunch times.
- I will not search for, view, download, upload or transmit any explicit or inappropriate material when using the internet.
- I will not share school-related passwords with pupils, staff or third parties unless permission has been given for me to do so.
- I will not install any software onto school ICT systems unless instructed to do so by the e-safety co-ordinator or Headteacher.
- I will only use recommended removable media, and will keep this securely stored.
- I will provide removable media to the e-safety officer for safe disposal once I am finished with it.

2. **Mobile devices**

- I will only use school-owned mobile devices for educational purposes.
- I will only use personal mobile devices during out-of-school hours, including break and lunch times.

- I will ensure that mobile devices are either switched off or set to silent mode during school hours, and will only make or receive calls in specific areas, e.g. the staffroom.
- I will ensure mobile devices are stored out of reach in a secure location during lesson times.
- I will not use mobile devices to take images or videos of pupils or staff – I will seek permission from the Headteacher before any school-owned mobile device is used to take images or recordings.
- I will not use mobile devices to send inappropriate messages, images or recordings.
- I will ensure that personal and school-owned mobile devices do not contain any inappropriate or illegal content.
- I will not access the WiFi system using personal mobile devices, unless permission has been given by the Headteacher or e-safety co-ordinator.
- I will not use personal and school-owned mobile devices to communicate with pupils or parents.
- I will ensure that any school data stored on personal mobile devices is password protected, and give permission for the e-safety officer to erase and wipe data off my device if it is lost or as part of exit procedures.

3. Social media and online professionalism

- If I am representing the school online, e.g. through blogging, I will express neutral opinions and will not disclose any confidential information regarding the school, or any information that may affect its reputability.
- I will not use any school-owned mobile devices to access social networking sites, unless it is beneficial to the material being taught; I will gain permission from the Headteacher before accessing the site.
- I will not communicate with pupils or parents over personal social networking sites.
- I will not accept ‘friend requests’ from any pupils or parents over social networking sites.
- I will ensure that I apply the necessary privacy settings to my social networking sites.
- I will not publish any comments or posts about the school on my social networking sites which may affect the school’s reputability.
- I will not post or upload any defamatory, objectionable, copyright infringing or private material, including images and videos of pupils, staff or parents, on any online website.
- I will not give my home address, phone number, mobile number, social networking details or email addresses to pupils or parents – any contact with parents will be done through authorised school contact channels.

4. Training

- I will ensure I participate in any e-safety or online training offered to me, and will remain up-to-date with current developments in social media and the internet as a whole.
- I will ensure that I allow the e-safety co-ordinator to undertake regular audits in order to identify any areas of need I may have in relation to training.
- I will ensure I employ methods of good practice and act as a role model for pupils when using the internet and other digital devices.
- I will ensure that I deliver any training to pupils as required.

5. **Reporting misuse**

- I will ensure that I adhere to any responsibility I have for monitoring, as outlined in the E-Safety Policy, e.g. to monitor pupils' internet usage.
- I will ensure that I report any misuse by pupils, or by staff members breaching the procedures outlined in this agreement, to the E-safety co-ordinator.
- I understand that my use of the internet will be monitored by the e-safety co-ordinator and recognise the consequences if I breach the terms of this agreement.
- I understand that the Headteacher may decide to take disciplinary action against me in accordance with the Allegations of Abuse Against Staff Policy, if I breach this agreement.

I certify that I have read and understood this agreement, and ensure that I will abide by each principle.

Signed: Date:

Print name:

Signed Headteacher: Date:

Print name:

2d - Acceptable Use Agreement – parents/carers

Technology Acceptable Use Agreement – Parents/Carers

Background

Technology has transformed learning, entertainment and communication for individuals and for all organisations that work with young people. However, the use of technology can also bring risks. All users should have an entitlement to safe internet

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

Parent's signature:	
Date:	

Permission to publish my child's work (including on the internet)

It is our school's policy, from time to time, to publish the work of pupils by way of celebration. This includes on the internet; via the school website and in the school's learning platform.
As the parent /carer of the above child I give my permission for this activity.

Parent's signature:	
Date:	

Permission for my child to participate in video-conferencing

Video-conferencing technology is used by the school in a range of ways to enhance learning – for example, by linking to an external "expert", or to an overseas partner school. Video conferencing only takes place under teacher-supervision. Independent pupil use of video-conferencing is not allowed.
As the parent / carer of the above child I give my permission for this activity.

Parent's signature:	
Date:	

The school's E-safety Policy, which contains this Acceptable Use Agreement, and the one signed by your child (to which this agreement refers), is available on the school website.

Appendix 3 - Guidance for Reviewing Internet Sites

This guidance is intended for use when the school needs to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might typically include cyber-bullying, harassment, anti-social behaviour and deception. These may appear in emails, texts, social networking sites, messaging sites, gaming sites or blogs etc.

Do not follow this procedure if you suspect that the web site(s) concerned may contain child abuse images. If this is the case please refer to the Flowchart for responding to online safety incidents and report immediately to the police.

Please follow all steps in this procedure:

- 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. *This will automatically be done for you if you are using Policy Central from Forensic Software or other monitoring software.* It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated, the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action
- If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of ‘grooming’ behaviour
    - the sending of obscene materials to a child
    - isolate the computer in question as best you can. Any change to its state may affect a later police investigation.
- It is important that all of the above steps are taken as they will provide an evidence trail for the group, possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

Sample documents for recording the review of and action arriving from the review of potentially harmful websites can be found in the PDF version of the SWGfL template e-safety policy (pages 36-38): http://www.swgfl.org.uk/Files/Documents/esp_template_pdf

Appendix 4 – Criteria for website filtering

A. ORIGIN - What is the website's origin?

- The organisation providing the site is clearly indicated.
- There is information about the site's authors ("about us", "our objectives", etc.)
- There are contact details for further information and questions concerning the site's information and content.
- The site contains appropriate endorsements by external bodies and/or links to/from well-trusted sources

B. CONTENT - Is the website's content meaningful in terms of its educational value?

- The content is age-appropriate
- The content is broadly balanced in nature, and does not appear unduly biased, partisan or unreliable
- The site is free of spelling mistakes, grammatical errors, syntax errors, or typos.
- **The site promotes equal and just representations of racial, gender, and religious issues.**
- **The site does not contain inappropriate content such as pornography, abuse, racial hatred and terrorism.**
- **The site does not link to other sites which may be harmful / unsuitable for the pupils**
- The content of the website is current.

C. DESIGN - Is the website well designed? Is it / does it:

- appealing to its intended audience (colours, graphics, layout)?
- easy to navigate through the site - links are clearly marked etc?
- have working links?
- have inappropriate adverts?

D. ACCESSIBILITY - Is the website accessible?

- Does it load quickly?
- Does the site require registration or passwords to access it?
- Is the site free from subscription charges or usage fees?

Appendix 5 - Supporting resources and links

The following links may help those who are developing or reviewing a school e-safety policy.

General

South West Grid for Learning “SWGfL Safe” - http://www.swgfl.org.uk/Staying-Safe
Child Exploitation and Online Protection Centre (CEOP) http://www.ceop.gov.uk/
ThinkUKnow http://www.thinkuknow.co.uk/
ChildNet http://www.childnet-int.org/
InSafe http://www.saferinternet.org/ww/en/pub/insafe/index.htm
Byron Reviews (“Safer Children in a Digital World”) - http://www.education.gov.uk/ukccis/about/a0076277/the-byron-reviews
Becta – various useful resources now archived
http://webarchive.nationalarchives.gov.uk/20101102103654/http:/www.becta.org.uk
London Grid for Learning - http://www.lgfl.net/esafety/Pages/education.aspx?click-source=nav-esafety
Kent NGfL http://www.kented.org.uk/ngfl/ict/safety.htm
Northern Grid - http://www.northerngrid.org/index.php/resources/e-safety
National Education Network NEN E-Safety Audit Tool - http://www.nen.gov.uk/hot_topic/13/nen-e-safety-audit-tool.html
WMNet – http://www.wmnet.org.uk
WES Worcestershire E-Safety Site – http://www.wes.networcs.net
EU kids Online http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx
Keeping Safe in Education - https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

Cyber Bullying

Teachernet “Safe to Learn – embedding anti-bullying work in schools” (Archived resources)
http://tna.europarchive.org/20080108001302/http://www.teachernet.gov.uk/wholeschool/behaviour/tacklingbullying/cyberbullying/
Anti-Bullying Network - http://www.antibullying.net/cyberbullying1.htm
Cyberbullying.org - http://www.cyberbullying.org/
East Sussex Council - Cyberbullying - A Guide for Schools:
https://czone.eastsussex.gov.uk/supportingchildren/healthwelfare/bullying/Pages/eastsussexandnationalguidance.aspx
CyberMentors: young people helping and supporting each other online - http://www.cybermentors.org.uk/

Social networking

Digizen – “Young People and Social Networking Services”:
http://www.digizen.org.uk/socialnetworking/
Ofcom Report: Engaging with Social Networking sites (Executive Summary)
http://www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/socialnetworking/summary/
Connect Safely - Smart socialising: http://www.blogsafety.com

Mobile technologies

“How mobile phones help learning in secondary schools”:

http://archive.teachfind.com/becta/research.becta.org.uk/upload-dir/downloads/page_documents/research/lsri_report.pdf

“Guidelines on misuse of camera and video phones in schools”
http://www.dundeecity.gov.uk/dundeecity/uploaded_publications/publication_1201.pdf

Data protection and information handling

Information Commissioners Office - Data Protection:

http://www.ico.gov.uk/Home/what_we_cover/data_protection.aspx

See also Becta (archived) resources above

Parents’ guide to new technologies and social networking

http://www.iab.ie/

Links to other resource providers

SWGfL has produced a wide range of information leaflets and teaching resources, including films and video clips – for parents and school staff. A comprehensive list of these resources (and those available from other organisations) is available on the “SWGfL Safe” website: http://www.swgfl.org.uk/staying-safe

BBC Webwise: http://www.bbc.co.uk/webwise/
Kidsmart: http://www.kidsmart.org.uk/default.aspx
Know It All - http://www.childnet-int.org/kia/
Cybersmart - http://www.cybersmartcurriculum.org/home/
NCH - http://www.stoptextbully.com/
Chatdanger - http://www.chatdanger.com/
Internet Watch Foundation: http://www.iwf.org.uk/media/literature.htm
Digizen – cyber-bullying films: http://www.digizen.org/cyberbullying/film.aspx
London Grid for Learning: http://www.lgfl.net/esafety/Pages/safeguarding.aspx?click-source=nav-toplevel

Appendix 6 - Glossary of terms

AUA	Acceptable Use Agreement – see templates earlier in this document
Becta	British Educational Communications and Technology Agency (former government agency which promoted the use of information and communications technology – materials and resources are archived and still relevant)
CEOP	Child Exploitation and Online Protection Centre (part of UK Police), dedicated to protecting children from sexual abuse. Providers of the Think U Know programmes.
DfE	Department for Education
FOSI	Family Online Safety Institute
ICT	Information and Communications Technology
ICT Mark	Quality standard for schools provided by NAACE for DfE
INSET	In-service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
IWF	Internet Watch Foundation
JANET	Provides the broadband backbone structure for Higher Education and for the National Education Network and Regional Broadband Consortia
KS1; KS2	KS1 = years 1 and 2 (ages 5 to 7) KS2 = years 2 to 6 (age 7 to 11)
LA	Local Authority
LAN	Local Area Network
Learning platform	An online system designed to support teaching and learning in an educational setting
LSCB	Local Safeguarding Children Board
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (eg WMNet) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
Ofsted	Office for Standards in Education, Children's Services and Skills
PDA	Personal Digital Assistant (handheld device)
PHSE	Personal, Health and Social Education
SRF	Self Review Framework – a tool maintained by Naace used by schools to evaluate the quality of their ICT provision and judge their readiness for submission for the ICTMark
SWGfL	South West Grid for Learning – the Regional Broadband Consortium of SW Local Authorities and recognised authority on all matters relating to e-safety (on whose policy this one is based)
URL	Universal Resource Locator – a web address
WMNet	The Regional Broadband Consortium of West Midland Local Authorities – provides support for all schools in the region and connects them all to the National Education Network (Internet)
WSCB	Worcestershire Safeguarding Children Board (the local safeguarding board)