E-Safety Policy:
The Chantry School

School Details: The Chantry School

Safeguarding Governor: Pat Owen

Designated Safeguarding Lead: Matt Lake Assistant Head

Deputy Safeguarding Lead: Jon Hill Year Head / Nicola Clear

Nominated Teacher in charge of safety: Jan Dowding

Ratified by Governing Body on: 13th September 2016 (as part of Safeguarding Policy)

Reviewed and amended September 2017

Next review date: September 2018

Contents

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 and young people, who are generally much more open to developing technologies than many adults. In many areas, technology is transforming the way that children and young people learn and are taught. At home, technology is changing the way children and young people 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.
- The potential to be drawn into terrorism through radicalisation via social media

This policy sets out how we strive to keep pupils safe with technology while they are in school. We recognise that children and young people are often more at risk when using technology at home (where often no controls over the technical structures are put in place to keep them safe) and so this policy also sets out how we educate them about the potential risks and try to embed appropriate behaviours.

Our e-safeguarding policy has been written from a template provided by Worcestershire County Council which has itself been derived from that provided by the South West Grid for Learning.

Section A - Policy and leadership

A.1.1 Responsibilities: the e-safety committee

Our school has an e-safety committee lead by our e-safety coordinator, J Dowding, and made up of pupils, our e-safety governor, the safeguarding lead or deputy and the Network Administrator. It meets on a termly basis to:

- Review and monitor this e-safety policy.
- Consider any issues relating to school filtering (see section B.2.1 of this policy)
- Discuss any e-safety issues that have arisen and how they should be dealt with.

Issues that arise are referred to other school bodies as appropriate and, when necessary, to bodies outside the establishment, such as the Worcestershire Safeguarding Children Board.

A.1.2 Responsibilities: governors

Governors are responsible for the approval of this policy as part of the safeguarding 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.

A.2.1 Illegal or inappropriate activities and related sanctions

The school believes that the activities listed below are inappropriate in an education 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, transfer data, 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 including radicalisation as per the Prevent Agenda (or hatred on the grounds of sexual orientation) (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

It is likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse in line with the pupil behaviour policy and the staff disciplinary policy. 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.2.2 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, irresponsible or, very rarely, through deliberate misuse.

Any e-safety breaches concerning staff should be reported to the lead teacher and pupils to the safeguarding lead or deputy.

Particular care should be taken if any apparent or actual misuse appears to involve illegal activity listed in section A.2.1 of this policy.

A.3.1 Use of hand held technology (personal phones and other 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 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
  - ✓ A school mobile phone is available for all professional use (for example when engaging in off-site activities). Members of staff should **not** use their personal device for school purposes except in an emergency.
- Pupils are not currently permitted to bring their personal hand held devices (for example tablet or laptop computers) into school. If these are required for an out of lesson activity, signed permission from parents/guardians is required.
- A number of such devices are available in school and are used by pupils as considered appropriate by members of staff.

	Staff / adults	Pupils

Personal hand held technology	Allowed	Allowed for selected staff	Not allowed	Allowed	Allowed with staff	Not allowed
Mobile phones may be brought into the school	✔			✔		
Use of mobile phones in lessons			✔			✔
Use of mobile phones in social time	✔					✔
Taking photos on personal phones or other camera devices			✔			✔
Use of hand held devices e.g. PDAs, gaming consoles	✔				✔	

A.3.2 Use of communication technologies

A.3.2a - Email

Access to email is provided for all teachers using Worcestershire schools' broadband via their Global IDs. Access to email is provided for all pupils through their Office365 ID.

- Staff and pupils should use only the school email services to communicate with others regarding school business when in school, or on school systems (e.g. by remote access)
- Users need to be aware that email communications may be monitored
- 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)
- Users must immediately report to their teacher the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature. They must not respond to any such email.

	Staff / adults				Pupils			
Use of Email	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff	Not allowed
Use of personal email accounts in school / on school network	✔						✔	
Use of school email for personal emails				✔				✔

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

	Staff / adults	Pupils

Use of social networking tools	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

Videoconferencing equipment in classrooms must be switched off when not in use and not set to auto answer.
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 teacher before making or answering a videoconference call.
Permission for pupils to take part in video conferences is sought from parents / carers at the beginning of the pupil's time in the school. Only where permission is granted may pupils participate.

A.3.3 Use of web-based publication tools

A.3.3a - Website (and other public facing communications)

Our school uses the public facing website (www.chantryschool.com) only for sharing information with the community beyond our school. This includes, from time-to-time, celebrating work and achievements of pupils. 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).
- 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 in association with photographs
  - ✓ written permission from parents or carers will be obtained before photographs of pupils are published on the school website
- Pupil's work can only be published with the permission of the pupil and parents or carers.

A.3.4 Professional standards for staff communication

In all aspects of their work in our establishment, teachers abide by the broad **Professional Standards for Teachers** laid down by the TDA 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, learning platform, 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.

Section B. Infrastructure

B.1 Password security

This is dealt with in detail in our school's Information Security Policy. 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.

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. No filtering system can, however, provide a 100% guarantee that it will do so. It is therefore important that the school has a filtering policy 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 procured by Worcestershire County Council, we automatically receive the benefits of a managed filtering service, with some flexibility for changes at local level.
The school also uses Policy Central monitoring software to check for inappropriate content or searches on user accounts.

B.2.1b - Responsibilities

The day-to-day responsibility for the management of the school's filtering policy is held by the **safeguarding coordinator** (with ultimate responsibility resting with the **head teacher and governors**). They manage filtering in line with this policy and keep logs of breaches of the filtering system.
All users have a responsibility to report immediately to teachers any infringements of the 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 e-safety education programme.
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 network administrator.

THEN

- The network administrator makes a request to IBS Schools Broadband Team
- The team will endeavour to unblock the site within a reasonable time. This process can take a number of hours so teaching staff are required to check websites well in advance of teaching sessions.

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 network and on school equipment. Monitoring takes place as follows:

- The network administrator monitors console captures weekly.
- 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.

Section 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 constant help and support to recognise and avoid e-safety risks and build their resilience. This is particularly important for helping them to learn how 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 Computing lessons in Years 7, 8 and 9 and during CPSE and form time. This is regularly revisited, covering the use of ICT and new technologies both in and beyond the school.
- 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 pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use of ICT both within and outside the school.
- 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 pupils to discuss anything of which they are unsure and implementing the expected sanctions and/or support as necessary.

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
  - ✓ 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

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

It is our general policy to encourage pupils to play a leading role in shaping the way our school operates and this is very much the case with our e-learning strategy. Pupils often use technology out of the school in ways that we do not in education and members of staff are always keen to hear of their experiences and how they feel the technology (especially rapidly developing technology such as mobile devices) could be helpful in their learning.
Pupils play a part in monitoring this policy (see section A.1.1).

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:

- It is expected that some staff will identify e-safety as a training need within the performance management process.
- All new staff should receive e-safety advice as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements, which are signed as part of their induction.
- The E-safety Co-ordinator (or another member of staff such as the Safeguarding Officer) will be CEOP trained.
- 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 appropriately qualified persons when required.

C.3 Governor training

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any subcommittee or group 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.

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 their 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, website
- Parents evenings