Victoria Primary School

E Safeguarding Policy

Updated March 2016

Background

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.
The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.
However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- 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 including prejudiced-based 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 use which may impact on the social and emotional development and learning of the young person.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The E Safeguarding Committee

Jackie Renton – E Safeguarding Leader / Assistant Head / ICT Leader / Named Person

Lynn Clews – Lead Named Person / Deputy Head

Jane Dark – Named Person / Headteacher

Our school technician is Mohammed Saleem. The committee will consult him over technical issues related to safeguarding and security of data.

The Pupil E Safety Champions

Year 6 – Zeeshaan Hussain, Husna Barakah

Year 5 – Hasnain Ali, Ameena Khan

Year 4 – Aminul Hoque, Humaina Mahmood

Year 3 – Taaha Basharat, Aminah Javaid

Development and Review of this policy.

This e-safeguarding policy was reviewed by the Governors School Improvement Committee	14.03.16
The implementation of this e-safety policy will be monitored by the:	Governors School Improvement Committee
Monitoring will take place at regular intervals:	Annually
The E-Safeguarding Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	March 2017
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	Children's services 01274 437500 (or 01274 431010 out of hours team) Bradford Learning Network – 01274 434825 Police Javelin House Child Protection Unit 01274 376061

Monitoring the impact of the policy

The school will monitor the impact of the policy using:

- Logs of reported incidents in the e-safeguarding incident log kept in the E safeguarding Leader's office
- Internal monitoring data for network activity (Jackie Renton – ICT Leader / Assistant Head)
- Smoothwall monitoring of network activity
- E-safety meetings
- E-Safe a forensic monitoring service monitors the school network. The E-safety leader Jackie Renton receives emails weekly to report on any inappropriate activity, or not, on any computer in school. Any activity report is followed up immediately.

Student E safeguarding data will be gathered at the beginning of 2016 through the use of the Bradford Council Children's Services eSafeguarding questionnaire available at: http://bradfordschools.net/limesurvey/ . Progress will be monitored at the start and the end of each academic year. As this policy is reviewed in March 2016 the first use of the survey will be in Autumn 2016.

Roles and Responsibilities

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors School Improvement Committee receiving regular information about e-safety incidents and monitoring reports

The Governors responsible for child protection and Safeguarding, including E safeguarding are Sandra Firm and Waheed Ali.

The role of these governors will include:

- regular meetings – which will include Safeguarding where e safety issues will be discussed
- regular monitoring of e-safety incident logs – forensic science software logs
- reporting to relevant Governors through minutes of the School Improvement Committee

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Leader Jackie Renton.
- The Headteacher / Senior Leaders are responsible for ensuring that the E-Safety Coordinator / Officer and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

- The Headteacher and E Safeguarding leader are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. This is detailed in the Child Protection Policy.

E-Safeguarding Leader:

- Takes day to day responsibility for e-safeguarding issues and has a leading role in establishing and reviewing the school e-safeguarding policy.

- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.

- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,

- Attends the Governors School Improvement Committee (which discusses e-safeguarding issues).

- Trains staff on E-safeguarding annually as part of child protection training

Network Manager / Technical staff:

Mohammed Saleem the school technician ensures:

- That the school's ICT infrastructure is secure and is not open to misuse or malicious attack

- That he keeps up to date with e-safety technical information and updates the E Safety leader or ICT coordinator as relevant

- That monitoring software and anti-virus software is implemented and updated

Teaching and Support Staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety policy

- They have an understanding of when to make referrals when there are issues concerning sexual exploitation, radicalisation and/or extremism

- They understand the risks posed by adult learners who use technology, including the internet, to bully, groom, radicalise or abuse children or learners

- They know where to seek professional advice and support

- They have read, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP)

- They report any suspected misuse or problem to the E-Safety leader for investigation

- Digital communications with students / pupils (eg email) should be on a professional level and only carried out using official school systems

- E-safety issues are embedded in all aspects of the curriculum and other school activities. E Safety lessons are taught through the Bradford Digital Literacy scheme.

- E-safety lessons are planned and taught every half term and that the lessons are age appropriate / reflect the needs of the age group

- Students / pupils understand and follow the school e-safety and acceptable use policy

- They are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices

- Any confidential files sent by email are saved in an encrypted file and the password for this file remains confidential

Named person for child protection

Lynn Clews (DHT), Jane Dark (HT) and Jackie Renton (AHT) are the Named people for child protection. They are trained in e-safety issues and are aware of the potential for serious child protection issues to arise from:

- sharing of personal data

- access to illegal / inappropriate materials

- inappropriate on-line contact with adults / strangers

- potential or actual incidents of grooming

- cyber-bullying, including prejudiced-based bullying

- radicalisation and extremist behaviour

- child sexual exploitation and trafficking

- the impact of new technologies on sexual behaviour, eg sexting

- Online safety and other associated issues

Children

- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems.

- Pupils are encouraged through E-Safety/PSHE lessons to share any E-Safety concerns with a trusted adult

- Are taught to learn to understand, respond to and calculate risk effectively

Parents / Carers

The school will take every opportunity to help carers / parents to understand issues related to e safety. We will assist parents to understand key issues in the following ways:
A parents e safety presentation delivered by local community police on an annual basis.
There will be an e safety element to the parents' meetings which take place half termly.
Regular newsletters offer parents advice on the use of the internet and social media at home.
Parents are asked to discuss the pupil Acceptable use policy with their children and are expected to sign their child's diary to say they have done so.

Community Users

Community Users/ visitors and volunteers will inform the Headteacher, Deputy Head or Assistant Head of any web sites they wish to access. No person can log on to the internet without a user account or the Internet password.

Education – Pupils

The education of pupils in e-safety is 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.

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

- A planned e-safety programme is delivered as part of PHSE in the form of the Bradford Digital Literacy Scheme.

- The Bradford ICT Scheme of work also highlights e-Safeguarding issues that arise in the context of ICT lessons.

- Key e-safety messages are reinforced as part of a planned programme of assemblies. They take place at least once a term.

- Pupils are taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information. Validation of information is covered in the research strand of the Bradford ICT scheme of work.

- Rules for the use of ICT systems will be posted in all rooms and displayed on log-on screens. Students will sign a copy of the Acceptable Use Policy and will be displayed in classrooms.

- For directed searches in school, staff direct children to an appropriate search engine or other search tools recommended in the research section of the Bradford ICT Scheme of work.

- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet. Copyright free audio and image sources are detailed in the Multimedia and Sound strands of the Bradford ICT scheme of work which the school follows.

Education - Staff Training

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:
A Staff meeting covering e safety will take place annually. This will be delivered by a member of Bradford Council Children's Services Curriculum ICT Team or the E Safeguarding Leader.
E safeguarding forms part of the annual child protection training received by all staff.
An audit of the e-safety training needs of all staff will be carried out regularly.
All new staff receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies.
The e-safeguarding leader has been trained as a ThinkUKnow Trainer. They are qualified to deliver CEOP Think U Know sessions to children and will receive regular updates on practice through the CEOP web site.

Education - Governor Training

Governors should take part in e-safety training / awareness sessions. Governors are invited to child protection and radicalisation training to enable them to keep informed. This may be delivered by Bradford Children's Services consultants or by the e-safeguarding leader.

Internet Provision

The school Internet is provided by the Bradford Learning Network, a DFE accredited educational internet service provider. All sites are filtered using the Smoothwall filtering system which also generates reports on user activity.

Use of digital and video images - Photographic, Video

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images online.

- Staff are allowed to take digital / video images to support educational aims. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.

- Photographs of children published on the website or blog must not contain full names.

- Pupils' full names will not be used anywhere on a website or blog.

- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website.

Personal Data Protection

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.

- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.

- Transfer data using encryption and secure password protected devices such as memory sticks.

Passwords

All users (adults and young people) will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
Passwords for new users, and replacement passwords for existing users can be allocated by Jackie Renton and Mohammed Saleem.
Members of staff will be made aware of the school's password policy:

- at induction

- through the school's e-safety policy and password security policy

- through the Acceptable Use Agreement

Pupils / students will be made aware of the school's password policy:

- in ICT and / or e-safety lessons (the school should describe how this will take place)

- through the Acceptable Use Agreement

All users will be provided with a username and password by Jackie Renton or Mohammed Saleem who will keep an up to date record of users and their usernames.

Management of assets

All ICT assets are recorded on an inventory spreadsheet. Assets that are damaged or surplus to requirements have data removed by the Technician before being collected and destroyed by a reputable company. Certificates are received and filed where this has taken place.

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT. However there may be incidents when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

If apparent or actual misuse appears to involve illegal activity such as:

- Child sexual abuse images
- Adult material which breaches the Obscene Publications Act

- Criminally racist material
- Other criminal conduct, activity or materials

Then staff should immediately follow the guidance highlighted in 'Actions upon discovering inappropriate or illegal material'. It is important that the device is not shut down as evidence could be erased but that it is removed to secure site. All matters should be reported immediately to the Head/E-Safety Coordinator.

If misuse has taken place which is not illegal it is important that any incidents are dealt with 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.

Whilst it is impossible to record possible sanctions for every eventuality a list of types of misuse and sanctions are included in the appendix to this policy.

Cyber bullying including prejudiced based bullying

Cyber bullying is the use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature. Examples of electronic communication are social networking web sites and apps, texting, use of other mobile or tablet apps, email or online software.
Pupils are taught about cyber bullying through E-Safety and PSHE lessons. Pupils are encouraged to share concerns of cyber bullying with a trusted adult. The adults in school will support the child by:

- Collecting evidence of the bullying taking place by recording the date, time and where possible screen captures
- Advising the child not to forward on messages to other people as this will continue the bullying
- Advising the child not to reply to the messages

Full details of how the school manages incidences of bullying can be found in our Anti-Bullying policy. The school may report serious cyber bullying incidents to the Police.

Social Media

Victoria Primary School uses Social Media in the following ways:

- A Text to Parents system which is managed by the school office. This is used as a reminder service for parents.
- As part of our school website pupils have a blog they can contribute to. All comments and posts are moderated by teachers before they are published. Pupils know that they must not share personal information on the blog or use it to communicate with people they do not know in real life.

All members of staff must keep their personal and professional lives separate on social media. Personal opinions should never be attributed to the school. The *school's* use of social media for professional purposes will be checked regularly by the E-Safety committee to ensure compliance with this policy.

Mobile devices

Staff

Staff must not use mobile phones in lessons. During teaching time, while on playground duty and during meetings, mobile phones will be switched off or put on 'silent' or 'discreet' mode. Except in urgent or exceptional situations, mobile phone use is not permitted during teaching time, while on playground duty and during meetings. Mobile phones should be kept in lockers and not carried around school, with the exception of the senior leadership team who are required to carry their phones for emergency purposes. In accordance with the Acceptable Use Policy staff should not use personal devices for photography in school. Only School cameras or devices are to be used.

Pupils

School does not allow children to bring mobile phones into school. As part of the digital literacy scheme of work we use pupils are taught about the dangers of using mobile phones, the fact that location services can say exactly where you are and how quickly children can post content online before thinking about the consequences.

School mobile devices

The school has a variety of mobile devices including iPods, iPads, Hudls, flip cams, digital cameras and laptops. All of the statements included in the Acceptable Use Policy apply to these mobile devices. Pupils know that they must not take pictures of other people without their permission. They are not allowed to download or install apps on any device. These devices are subject to the same levels of internet filtering as all the school computers accessed by children.

We have detailed Acceptable Use Policies for staff and pupils and a separate Acceptable use of cameras and mobile phones policy. This is included in the appendix of this policy.

Development and Review of this policy

The implementation of this policy will be monitored by the E-Safeguarding Committee.

Monitoring of the policy will take place annually, or more regularly in light of any significant new developments in the use of technologies, new threats to E-Safety of incidents that have taken place.

Should serious E-Safety incidents take place, the following external persons/agencies should be informed: Initial Contact point Children's Services, Bradford Learning Network, Police Child Protection Unit.

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound. (Regulation of Investigatory Powers Act 2000).

Victoria Primary School
Acceptable use of cameras & mobile phones policy

School Mission Statement

Victoria Primary School is a safe, caring and aspirational learning environment, where everyone respects each other. We work in partnership to ensure each child achieves their full potential, has self-belief and is equipped for life.

Statement of intent

It is our intention to provide an environment in which children, parents and staff are safe from images being recorded and inappropriately used in turn eliminating the following concerns:
1) Staff being distracted from their work with children
2) The inappropriate use of mobile phone and cameras around children

Aim

Our aim is to:
Have a clear policy on the acceptable use of mobile phones and cameras that is understood and adhered to by all parties concerned without exception.
In order to achieve this aim, we operate the following Acceptable Use Policy:

Mobile Phones

Victoria Primary School allows staff to bring in personal mobile telephones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a current pupil or parent/carer using their personal device.
Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
Staff must ensure that their mobile telephones/devices are left inside their bag throughout contact time with children. Staff bags should be placed in a secure place within the classroom, staff room or locker.
The Senior Leadership team are required to carry their mobile phone with them in school in case of an emergency such as a fire or other serious incident that requires evacuation of the school site, (see Emergency Plan).
Mobile phone calls may only be taken at staff breaks or in staff members' own time.
If staff have a personal emergency they are free to use the school's phone or make a personal call from their mobile in the office or the staff room.
If any staff member has a family emergency or similar and required to keep their mobile phone to hand, prior permission must be sought from the Headteacher.
Staff (will need to) ensure that the Headteacher has up to date contact information and that staff make their families, children's schools etc. aware of emergency work telephone numbers. This is the responsibility of the individual staff member.
All parent helpers will be requested to place their bag containing their phone in a secure area or another appropriate location and asked to take or receive any calls in the staffroom or office.
During group outings nominated staff will have access to their mobile phone, which is to be used for communication with school as necessary or emergency purposes.

It is the responsibility of all members of staff to be vigilant and report any concerns to the Headteacher. Concerns will be taken seriously, logged and investigated appropriately (see allegations against a member of staff policy).
Mobile phones must not be used to take photographs of children.
Mobile phones must not be used to take photographs of children by parents in school or on school visits.

Cameras

School Cameras must be used. The memory card should then be removed and the content loaded onto a school computer not a personal computer. Photographs taken for the purpose of recording a child or group of children participating in activities or celebrating their achievements is an effective form or recording their progression.
Only the designated school cameras are to be used to take any photo within the school.
All staff are responsible for the location of the cameras and are responsible for ensuring they are stored securely.
The camera must be put away at the end of every session.
Images taken and stored on the camera must be downloaded as soon as possible on to a school computer, ideally once a week.
Failure to adhere to the contents of this policy could lead to disciplinary action being taken.
Photographs at school performances are not allowed. Opportunities are given to parents to take photographs of their own child at the end of any school performances.

Policy reviewed 14.03.16

Staff Acceptable Use Policy

ICT Acceptable Use Agreement for Staff

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this Acceptable Use Agreement. Members of staff should consult the school's e-Safeguarding Policy for further information and clarification.

I understand that my use of school information systems (e.g. SIMS), Internet (including email) and any other networked ICT resources will be monitored and recorded to ensure Policy compliance.

I will respect system security and I will not disclose any password or security information to anyone other than on request from an authorised system manager (including but not limited to the ICT Coordinator Business Manager and external technical support provider).

I will not install any software (including mobile apps) or hardware without permission from the ICT Coordinator.

I will ensure that pupil data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.

I will adhere to copyright and intellectual property laws and only publish media which I own, have permission to use or is copyright-free.

I will report any incidents of concern regarding children's safety whilst using new technologies in or out of school to the e-Safety leader.

I will ensure that electronic communications with pupils including blog comments are compatible with my professional role and that messages cannot be misunderstood or misinterpreted. I understand that befriending pupils on instant messaging services and social networking sites is prohibited.

I will not, on any instant messaging service or social networking site, behave in any manner that would or could bring the school into disrepute.

I will not use any personal device (including cameras and mobile phones) to capture images, videos or audio of pupils or to access social networking sites in school time.

I will promote e-Safety with pupils in my care and will help them to develop a responsible attitude to system use, communications and publishing.

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept email and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and accept the ICT Acceptable Use Agreement for Staff.

Name: …… Signed: …… Date: ……

Dealing with Online Safety Incidents

Action you must take if you discover inappropriate (threatening or malicious) material online concerning yourself or your school:

All online safety incidents are recorded in the School Online Safety Log which is regularly reviewed.

Any incidents where pupils do not follow the Acceptable Use Policy will be dealt with following the school's normal behaviour or disciplinary procedures.

In situations where a member of staff is made aware of a serious online safety incident concerning pupils or staff, they will inform the E Safeguarding Leader – Jackie Renton, or the Headteacher who will then respond in the most appropriate manner. Who will take the following steps:

- Secure and preserve any evidence. For example, note the web address (URL) or take a screen shot or copy and print the screen
- Inform the Named Person – Lynn Clews, Jane Dark or Jackie Renton
- If appropriate, inform the Police Child Protection Unit – Javelin House – 01274 376061
- If appropriate contact parents

Instances of **online bullying** will be taken very seriously by the school and dealt with using the school's anti-bullying procedures. School recognizes that staff as well as pupils may be victims and will take appropriate action in either situation, including instigating restorative practices to support the victim.

Incidents which create a risk to the security of the school network, or create an information security risk, will be referred to the school's E safeguarding Leader, Jackie Renton, and technician Mohammed Saleem, and appropriate advice sought and action taken to minimize the risk and prevent further instances occurring, including reviewing any policies, procedures or guidance. If the action breaches school policy then appropriate sanctions will be applied. The school will decide if parents need to be informed if there is a risk that pupil data has been lost.

School reserves the right to monitor equipment on their premises and to search any technology equipment, including personal equipment with permission, when a breach of this policy is suspected.

Dealing with a Child Protection issue arising from the use of technology:

If an incident occurs which raises concerns about child protection or the discovery of indecent images on the computer this must be immediately referred to the Headteacher and E safeguarding Leader. It is a criminal act under Section 1 of the Protection of Children Act 1978 for any person to make and distribute indecent images of children. These are arrestable offences.

Upon the receipt of any information concerning a person who is suspected of accessing indecent images of children online, their employer head should notify the Police (Child and Public Protection Unit) immediately. The computer should be left and not used by anyone, allowing this to be seized as evidence for forensic examination by the Police. The details of all persons having access to the computer should be made available to allow a clear evidence trail to be established.

Dealing with complaints and breaches of conduct by pupils:

- Any complaints or breaches of conduct will be dealt with promptly
- Responsibility for handling serious incidents will be given to a senior member of staff
- Parents and the pupil will work in partnership with staff to resolve any issues arising
- Restorative practice will be used to support the victims
- There may be occasions when the police must be contacted. Early contact will be made to establish the legal position and discuss strategies

The following activities constitute behaviour which we would always consider unacceptable (and possibly illegal):

- accessing inappropriate or illegal content deliberately
- deliberately accessing downloading and disseminating any material deemed inappropriate, offensive, obscene, defamatory, racist, homophobic, violent, promoting radicalization and/or extremism
- continuing to send or post material regarded as harassment or of a bullying nature after being warned
- staff using digital communications to communicate with pupils in an inappropriate manner (for instance, using personal email accounts, personal mobile phones, or inappropriate communication via social networking sites)

The following activities are likely to result in disciplinary action:

- any online activity by a member of the school community which is likely to adversely impact on the reputation of the school
- accessing inappropriate or illegal content accidentally and failing to report this
- inappropriate use of personal technologies (e.g. mobile phones) at school or in lessons
- sharing files which are not legitimately obtained e.g. music files from a file sharing site
- using school or personal equipment to send a message, or create content, that is illegal, offensive or bullying in nature or could bring the school into disrepute
- attempting to circumvent school filtering, monitoring or other security systems
- circulation of commercial, advertising or 'chain' emails or messages
- revealing the personal information (including digital images, videos and text) of others by electronic means (e.g. sending of messages, creating online content) without permission
- using online content in such a way as to infringe copyright or which fails to acknowledge ownership (including plagiarizing of online content)
- transferring sensitive data insecurely or infringing the conditions of the Data Protection Act 1998

The following activities would normally be unacceptable; in some circumstances they may be allowed e.g. as part of planned curriculum activity or by a system administrator to problem solve

- accessing social networking sites, chat sites, instant messaging accounts, email or using a mobile phone for personal use during school hours
- accessing non-educational websites (e.g. gaming or shopping websites)
- sharing a username and password with others or allowing another person to log in using your account
- accessing school ICT systems with someone else's username and password
- deliberately opening, altering, deleting or otherwise accessing files or data belonging to someone else