WOODFIELD
ACADEMY

E-safety Policy

WOODFIELD
ACADEMY

Approved on

25th January 2017

Signed by Chair of Governors

_____

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 truer 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. We also explain how we attempt to inform those people who work with our pupils beyond the academy environment (parents, friends and the wider community) to be aware and to assist in this process.

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

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 academy.

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: the e-safety committee

Our academy has an e-safety committee lead by our e-safety coordinator and made up of teachers and our e-safety governor. Pupils will have input to this group through their school council. The purpose of this group is to:

- Review and monitor this e-safety policy.
- Consider any issues relating to school filtering
- Discuss any e-safety issues that have arisen and how they should be dealt with.

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

A.1.2 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:

- Leads the e-safety committee.
- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the academy 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 academy technical staff.
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- Meets regularly with e-safety governor to discuss current issues and review incident logs.
- Attends relevant meetings and committees of Governing Body.
- Reports regularly to Senior Leadership Team.
- Receives appropriate training and support to fulfil their role effectively.

A.1.3 Responsibilities: governors

Governors are responsible for the approval of this policy and for reviewing its effectiveness. This will be carried out by the governors 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 with an agenda based on:*
    - *monitoring of e-safety incident logs*
    - *reporting to relevant Governors committee / meeting*

A.1.4 Responsibilities: head teacher

- The head teacher is responsible for ensuring the safety (including e-safety) of all members of the academy community, though the day to day responsibility for e-safety is delegated to the E-Safety Co-ordinator
- The head teacher and another member of the senior management team 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.

A.1.5 Responsibilities: Teaching and Support Staff

Teaching and Support Staff are responsible for ensuring that:

- They safeguard the welfare of pupils and refer child protection concerns using the proper channels: **this duty is on the individual, not the organisation or the academy**.
- They have an up to date awareness of e-safety matters and of the current academy e-safety policy and practices, including the school's approach to the Prevent Agenda.
- They are able to identify children who may be vulnerable to radicalisation, and know what to do when they are identified.
- They have read, understood and signed the academy'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 via email in a fully professional manner and only using official systems.
- They embed e-safety issues in the curriculum and other activities, also acknowledging the planned e-safety programme.

A.1.6 Responsibilities: Technical Staff

The technical staff are responsible for ensuring that:

- The academy's ICT infrastructure and data are secure and not open to misuse or malicious attack.
- The academy meets the e-safety technical requirements outlined.
- Users may only access the academy's networks through a properly enforced password protection policy.
- Shortcomings in the infrastructure are reported to the ICT coordinator or head teacher so that appropriate action may be taken.
- Monitoring software / systems are implemented and updated as agreed in school policies.
- Reviews the output from monitoring software and initiates action where necessary.
- They keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant

A.2.1 Policy development, monitoring and review

The academy e-safety policy has been developed by the

- E-Safety Coordinator
- Safeguarding Team
- Safeguarding officer

Consultation with the whole school community will take place through the following:

- Staff meetings
- School Council
- Governor's meeting
- Academy website

Schedule for development / monitoring / review of this policy

This e-safety policy was approved by the governing body on:	25th January 2017
The implementation of this e-safety policy will be monitored by the:	*The e-safety committee under the direction of the e-safety coordinator*
Monitoring of this policy will take place at regular intervals:	*Termly*
The governing body will receive regular reports on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) as part of a standing agenda item with reference to safeguarding:	*Twice per year*
The e-safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of technology, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	*January 2018*
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	*Worcestershire Safeguarding Children Board* *Local Authority Designated Officer* *Worcestershire Senior Adviser for Safeguarding Children in Education* *West Mercia Police*

A.2.2 Policy Scope

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

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 site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, radicalisation or other e-safety incidents covered by this policy, which may take place out of the academy, but are linked to membership of the academy.

The academy 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 academy.

A.2.3 Acceptable Use Agreements

All members of the academy community including technicians, whether directly employed or from external technical support teams, are responsible for using the academy ICT systems in accordance with the Acceptable Use Agreement (AUA), which they will be expected to sign before being given access to academy systems.

Acceptable Use Agreements are provided in Appendix 1 of this policy for:

- Pupils
- Staff (and volunteers)
- Community users of the academy's ICT system
- Technical support personnel

Acceptable Use Agreements are signed by all pupils as they enter the academy Pupils will re-sign on entering a new Key Stage. Parents will be asked to support their child's with understanding and the signing of the AUP

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

Parents sign once when their child enters the academy. Community users sign when they first request access to the academy's ICT system.

Induction policies for all members of the academy community include this guidance.

A.2.4 Self Evaluation

Evaluation of e-safety is an ongoing process and links to other self-evaluation tools used in the academy in particular pre Ofsted evaluations along the lines of the Self Evaluation Form (SEF).

A.2.5 Whole School approach and links to other policies

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

Core ICT policies

E-Safety Policy	How we strive to ensure that all individuals in academy stay safe while using Learning Technologies.
Data Security Policy	How we categorise, store and transfer sensitive and personal data and protect systems. This links strongly and overlaps with the e-safety policy.
Computing curriculum	Key documents and associated resources directly relating to learning covering the Computing Curriculum

Other policies relating to e-safety

Anti-bullying	How the academy strives to eliminate bullying
PSHE	E-Safety has links to staying safe
Safeguarding	Safeguarding pupils electronically is an important aspect of E-Safety. ***The e-safety policy forms a part of the academy'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 academy 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 academy 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)**
- 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 academy or brings the academy into disrepute

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

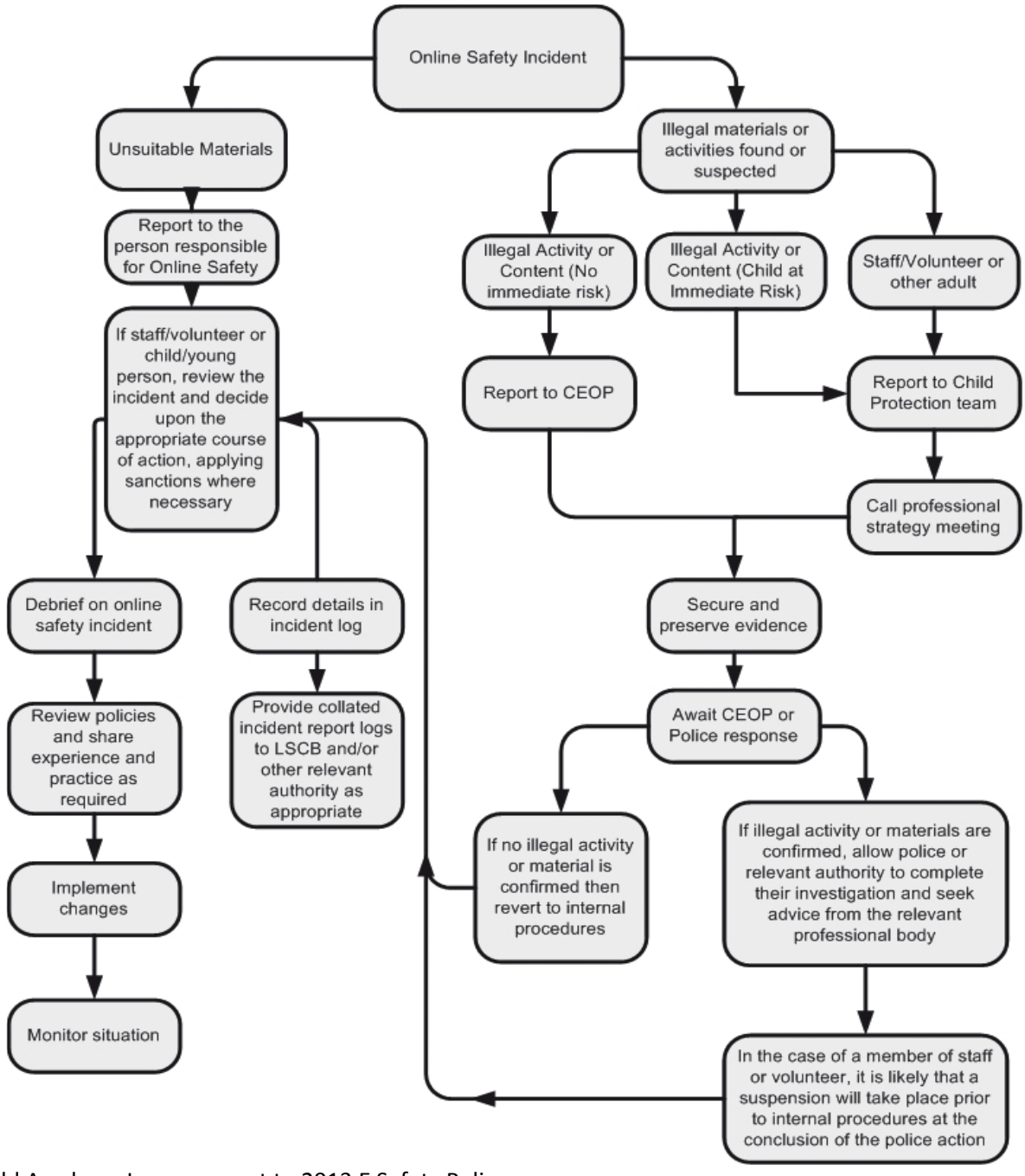
- *Using academy systems to undertake transactions pertaining to a private business*
- *Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Worcestershire County Council Broadband or the academy*
- *Uploading, downloading or transmitting commercial 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*
- *On-line shopping / commerce unless directly related to academy business*
- *Use of social networking sites*

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.

Any incidents will be dealt with as soon as possible in a **proportionate** manner, members of the academy 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 academy 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. Listed below are the responses that will be made to any apparent or actual incidents of misuse:



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 academy'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 should not be used in front of, or in the presence of students. Except in the case of emergency.*
  - ✓ *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.*
- *Pupils are not currently permitted to bring their personal hand held devices into lessons and must submit them to the office on arrival.*

A.3.2 Use of communication technologies

The use of communication technologies within the academy will be regularly reviewed and updated to ensure that all staff and students are complying with the policy and acting as effective digital citizens.

A.3.2a - Email

Access to email is provided for all through the academy.

These official academy email services may be regarded as safe and secure and are monitored.

- Staff and pupils should use only the academy email services to communicate with others regarding academy business.
- Users need to be aware that email communications may be monitored.
- *Pupils will ask for permission to communicate with people outside of the academy.*
- 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.
- 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.

A.3.2b - Social networking (including chat and instant messaging)

The use of social media, chat or instant messaging is not permitted on the academy system.

Training time for staff is allocated to ensure safe practice from home and advice given in Acceptable Use Policy (AUP)

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.
- Members of staff are allowed to take digital still and video images to support educational aims, but must follow policies concerning the sharing, distribution and publication of those images. Those images should only be captured using academy equipment; **the personal equipment of staff should not be used for such purposes.**
- 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 academy into disrepute.
- Staff should be aware of pupils for whom it has been deemed inappropriate to take and share/publish their photograph (e.g. some looked after children)
- Pupils must not take, use, share, publish or distribute images of others without their permission

A.3.4 Use of web-based publication tools

A.3.4a – School Website

Our school/academy uses the public facing website **http://www.woodfield.worcs.sch.uk** only for sharing information with the community beyond our academy. 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 academy 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 with parental permission..*
- Detailed calendars will not be published on the school/academy 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 academy website
- Pupil's work can only be published with the permission of the pupil and parents or carers. 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 academy systems.
- Personal email addresses, text messaging or public chat / social networking technology must not be used for these communications.

A.3.6 Use of Video Conferencing

Videoconferencing equipment in classrooms must be switched off when not in.

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

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

Videoconferencing will be supervised directly by a teacher.

Permission for pupils to take part in video conferences is sought from parents / carers before taking part in any Video conferencing

Only key administrators have access to videoconferencing administration areas.

Any Video conferencing should be done with attention to the Data Protection policy and any sensitive information must be communicated under strict privacy.

Section B. Infrastructure

B.1 Password security

The academy's e-safety curriculum will include frequent discussion of issues relating to password security and staying safe in and out of the academy

The academy will be responsible for ensuring that the *school infrastructure / network* is as safe and secure as is reasonably possible and that:

- Users can only access data to which they have right of access
- No user should be able to access another's files, without permission (or as allowed for monitoring purposes within the school's policies).
- Access to personal data is securely controlled in line with the academy data policy
- Logs are maintained of access by users and of their actions while users of the system

All students are issued a one-time password at the start of each academic year. All students then have the right to change their password at any time.

All users of the academy system are offered advice on secure passwords.

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. We therefore support this system with our own white / black list process.

B.2.1b - Responsibilities

The day-to-day responsibility for the management of the academy's filtering policy is held by the **Network Manager** (with ultimate responsibility resting with the **head teacher and governors**).

They manage filtering in line with this policy and keep logs of changes to and breaches of the filtering system.

All users have a responsibility to report immediately to the e-safety coordinator 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 academy's computing curriculum,

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

- Signing the Acceptable Use Agreement
- Briefing in staff meetings, training days, memos etc.

Parents will be informed of the academy'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 academy, the process to unblock is as follows:

- The teacher makes the request to the academy Network Manager
- The Network Manager checks the website content to ensure that it is appropriate for use in academy.
- *If agreed, the network manager will create the whitelist or apply to the county broadband provider to remove the block*

B.2.1e - Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The academy will therefore monitor the activities of users on the network and on academy equipment.

Monitoring takes place as follows:

- Monitoring consoles will be regularly checked for any inappropriate content.
- 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

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

- A planned e-safety programme is provided as part of Computing, This is regularly revisited, covering the use of ICT and new technologies both in and beyond the academy
- 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 academy.
- In lessons where internet use is pre-planned, it is best practice that younger pupils should be guided to sites checked as suitable for their use.
- Clear steps are in place for reporting inappropriate content
- 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.
- Pupils will be made aware of what to do should they experience anything, while on the Internet, which makes them feel uncomfortable.

C.1.2 Digital literacy

- Pupils will 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?)
    - ✓ Referring to other (including non-digital) sources
- Pupils will be taught 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 policy to encourage pupils to play a leading role in shaping the way our academy operates and this is very much the case with our e-learning strategy. Pupils often use technology out of the academy 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 will play a part in monitoring this policy

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:

- A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly.
- It is expected that some staff will identify e-safety as a training need within the performance management process.
- The E-safety Co-ordinator (or another member of staff such as the Safeguarding Officer) will be CEOP trained.
- All teaching staff will be expected to be aware of this policies content
- The E-Safety Coordinator will provide advice, guidance and training as required to individuals as required on an ongoing basis.

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.

The safeguarding governor works closely with the e-safety coordinator and reports back to the full governing body.

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.

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

- Letters, newsletters and web site,
- Parents evenings

C.5 Wider community understanding

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

Appendix 1 – Pupil Acceptable Use Agreement

Copy of this in the school diary

Rules for Responsible Internet Use

The school has installed computers with internet access to help our learning, these rules will help keep us safe, keep the network safe, and help us to be fair to others.

- **I will only access the system with my class username and password which I will keep secret.**
- **I will not access other pupils' files or folders without permission.**
- **I will only use the school computers for school work and homework.**
- **I will not use memory sticks at school unless they have been virus checked by a member of staff. I will also get permission to use them first.**
- **I will ask permission from a member of staff before using the internet and will not use it to play online games or download files.**
- **I will only email people I know or whom my teacher has approved.**
- **The messages I send will be polite and responsible.**
- **I will not give my home address or telephone number or arrange to meet someone, unless a parent, carer or teacher has given permission.**
- **I will report any unpleasant material or messages sent to me. II understand that this report would be confidential and would help protect other pupils and myself.**
- **If I find an internet site which is inappropriate, I will tell the teacher immediately. I will not tell other pupils about it.**
- **I understand that the school may check my computer files and emails, and may monitor the internet sites I visit.**
- **When using school equipment I will do so with care. I will report any damage equipment soon as I notice it.**
- **When using school digital cameras I will only take photos which are appropriate and relevant to the task set.**

Dear Parent/ Carer

ICT including the internet, e-mail and mobile technologies, has become an important part of learning in our school. We expect all children to be safe and responsible when using ICT.

Please read and discuss these E-Safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact your child's class teacher or Mr Smith.

Parent/ carer signature

We have discussed this and ……..(child name) agrees to follow the E Safety rules and to support the safe use of ICT at Woodfield Academy

Parent/ Carer Signature ……

Class …… Date ……

Appendix 2 – Staff Acceptable Use Policy

Acceptable Use Agreement: All Staff, Volunteers and Governors

Covers use of all digital technologies in school: i.e. **email, Internet, network resources**, software, communication tools, **equipment and systems.**

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will ensure all documents, data etc., are printed, saved, accessed and deleted / shredded in accordance with the school's data policy.
- I will not engage in any online activity or use social media in a way that may compromise my professional responsibilities.
- I will only use the approved email system(s) for any school business.
- I will not browse, download or send material that could be considered offensive to colleagues or children.
- I will report any accidental access to, or receipt of inappropriate materials to the network manager
- I will not download any software or resources from the Internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.
- I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.
- I will not connect any device (including USB flash drive), to the network that does not have up-to-date anti-virus software,
- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home.
- I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the *appropriate system or staff-only drive within school*.
- I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to are not confused with my professional role.
- I will ensure, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role.
- I agree and accept that the iPad loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use".
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will alert *a* senior member of staff if I feel the behaviour of any child that uses ICT in my presence, may be a cause for concern.
- I understand that it is my duty to support a whole-school safeguarding approach and will report any inappropriate use of ICT or social media immediately.
- I understand that all Internet and network traffic / usage can be logged.
- I will embed the school's e-safety / digital literacy curriculum into my teaching.

User Signature

I agree to abide by all the points above.

I understand that I have a responsibility for my own and others e-safeguarding and I undertake to be a 'safe and responsible digital technologies user'.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.

I understand that failure to comply with this agreement could lead to disciplinary action.

Signature ..... Date .....

Full Name ..... (printed)

Job title / Role .....

Authorised Signature (Head Teacher / Deputy)

I approve this user to be set-up on the school systems relevant to their role

Signature ..... Date .....

Full Name ..... (printed)

Appendix 3 - Permission for my child to use the internet and electronic communication

NAME OF PUPIL:	CLASS:

Data Protection Act 1988: The school is registered under the Data Protection Act for holding personal data. The school has a duty to protect this information and keep it up to date. The school is required to share some of the data with the Education Authority and with the DFE.

COPYRIGHT PERMISSION

I give permission for my child's work to appear in school documentation, on the website and in the media	**Yes**		**No**	

INTERNET ACCESS

I give permission for my child to have internet access in school	**Yes**		**No**	

PHOTOGRAPHS

The school regularly uses photographs and video for educational purposes, particularly recording achievements. On occasions these photographs are passed to the press for publicity. If you do not wish your child's picture to be passed to the press at any time you must express this in writing to the school. At all times the school will operate within the Data Protection Act.				
I give permission for my child's photograph to appear in school documentation, on the website and in the media	**Yes**		**No**	

I give permission for my child's full name to appear in school documentation, on the website and in the media	**Yes**		**No**	

SEX EDUCATION

Sex and Relationship Education is delivered in school as part of the Curriculum.

If you do not give permission for your son/daughter to take part in these lessons, please attach a letter outlining your reasons against, to this consent form.

DATA EXCHANGE

Your child's information may be passed on to external agencies. This will only be agencies with an official role in the Local Authority or local education system. At all times the school will operate within the Data Protection Act.

Appendix 4 - Acceptable Use Agreement – community user

You have asked to make use of our academy's ICT facilities. Before we can give you a log-in to our system we need you to formally agree to use the equipment and infrastructure responsibly.

For my professional and/or personal safety:

- I understand that the academy will monitor my use of the ICT systems, email and other digital communications.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, of which I become aware, to a member of the academy staff.

I will be responsible in my communications and actions when using the academy ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files or data, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.

The academy and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the academy:

- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist or radical material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others.
- I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials described above.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, except with the specific approval of the academy.
- I will not disable or cause any damage to academy equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

I have read and understand the above and agree to use the academy ICT systems (both in and out of the academy) within these guidelines. I understand that failure to comply with this agreement will result in my access to the academy's ICT systems being withdrawn, that further actions will be taken in the event illegal activity, and that I may be held liable for any damage, loss or cost to the academy as a direct result of my actions.

Community user Name:	
Signed:	
Date:	

Appendix 5 - Guidance for Reviewing Internet Sites

This guidance is intended for use when the academy 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 / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - 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.

Appendix 6 – 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 and 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 7 - 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 academy's 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 academy's 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 academies 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 academys in the region and connects them all to the National Education Network (Internet)
WSCB	Worcestershire Safeguarding Children Board (the local safeguarding board)

Appendix 8 - Reporting Log

Reporting Log

Group .....

Date	Time	Incident	Action taken		Incident Reported by	Signature
			What?	By whom?		

Appendix 9 Social Networking Whole School Agreement

For the protection of yourself, your school community and your establishment:

- Ensure that all your privacy settings are set to 'Friends Only'. Go to your Account Settings and make sure that the Custom Settings are highlighted and that these show that status, photos and posts are set to 'Friends Only'.

- Consider what information you have on your info page and your profile picture. Including brief information and an unidentifiable picture, e.g. sunset, will assist in making your profile indistinctive.

- Be careful what photographs you include on your profile. Once these are uploaded, they are very difficult to remove and, using image editing software, they can be altered and merged with other more distasteful images.

- If you have professional and social 'friends' on Facebook or other social networking sites, using the group list feature will ensure that you can distinguish what type of information you send to particular groups.

- Do not accept pupils (even those that have recently left the school), parents or carers as 'friends'.

- Do not use Facebook or other social networking sites in any way that might bring your professional status or your school into disrepute.

- Taking charge of your digital reputation is important, as unprofessional posts or images will lead to disciplinary action and possible failure to gain employment in the future.

- Do not post or upload photographs relating to colleagues, pupils or parents. Objection to such posts can cause friction in your school and make your working environment uncomfortable.

- Do not post or upload photographs related to school-based or extra-curricular activities and do not make specific reference to your school in any post as comments may be misconstrued and result in inappropriate responses.

- Be aware of any spam or potential virus risks sent via rogue posts. It is advisable to check with anti-virus firms if you get any suspicious requests or posts.

- If you are alerted to any negative or unscrupulous information about yourself, colleagues or your school on Facebook or other social networking sites, inform your headteacher. Further advice to help with cyberbullying incidents etc., can be gained from help@saferinternet.org.uk (0844 3814772) or a professional association such as your Trade Union.

- ***I understand the implications of using Facebook and other social networking sites for my own protection and professional reputation, as well as the impact that my use can have on my school community and establishment.***
- ***I understand that injudicious use of social networking may lead to disciplinary action.***
- ***I agree to take all possible precautions as outlined above.***

Name		***Date***	

Appendix 10 - Guidance for Reviewing Internet Sites

This guidance is intended for use when the academy 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 / volunteer 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.

Record of reviewing devices / internet sites (responding to incidents of misuse)

Group	
Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

Name and location of computer used for review (for web sites)

Web site(s) address / device	**Reason for concern**

Conclusion and Action proposed or taken

Black or White listing websites

If you feel that a website should be blocked or unblocked please3 complete the following.

Details of person who requested changes

Name	
Position	
Signature	

Technician performing change

Name	
Position	
Signature	

Date	
Website to block / unblock	
Nature of website	

SCHOOL COPY

Appendix 2 – Staff Acceptable Use Policy

Acceptable Use Agreement: All Staff, Volunteers and Governors

Covers use of all digital technologies in school: i.e. **email, Internet, network resources**, software, communication tools, **equipment and systems.**

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will ensure all documents, data etc., are printed, saved, accessed and deleted / shredded in accordance with the school's data policy.
- I will not engage in any online activity or use social media in a way that may compromise my professional responsibilities.
- I will only use the approved email system(s) for any school business.
- I will not browse, download or send material that could be considered offensive to colleagues or children.
- I will report any accidental access to, or receipt of inappropriate materials to the network manager
- I will not download any software or resources from the Internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.
- I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.
- I will not connect any device (including USB flash drive), to the network that does not have up-to-date anti-virus software,
- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home.
- I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the *appropriate system or staff-only drive within school*.
- I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to are not confused with my professional role.
- I will ensure, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role.
- I agree and accept that the iPad loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use".
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will alert *a* senior member of staff if I feel the behaviour of any child that uses ICT in my presence, may be a cause for concern.
- I understand that it is my duty to support a whole-school safeguarding approach and will report any inappropriate use of ICT or social media immediately.
- I understand that all Internet and network traffic / usage can be logged.
- I will embed the school's e-safety / digital literacy curriculum into my teaching.

User Signature

I agree to abide by all the points above.

I understand that I have a responsibility for my own and others e-safeguarding and I undertake to be a 'safe and responsible digital technologies user'.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.

I understand that failure to comply with this agreement could lead to disciplinary action.

Signature ..... Date .....

Full Name ..... (printed)

Job title / Role .....

Authorised Signature (Head Teacher / Deputy)

I approve this user to be set-up on the school systems relevant to their role

Signature ..... Date .....

Full Name ..... (printed)

Appendix 9 Social Networking Whole School Agreement

SCHOOL COPY

For the protection of yourself, your school community and your establishment:

- Ensure that all your privacy settings are set to 'Friends Only'. Go to your Account Settings and make sure that the Custom Settings are highlighted and that these show that status, photos and posts are set to 'Friends Only'.

- Consider what information you have on your info page and your profile picture. Including brief information and an unidentifiable picture, e.g. sunset, will assist in making your profile indistinctive.

- Be careful what photographs you include on your profile. Once these are uploaded, they are very difficult to remove and, using image editing software, they can be altered and merged with other more distasteful images.

- If you have professional and social 'friends' on Facebook or other social networking sites, using the group list feature will ensure that you can distinguish what type of information you send to particular groups.

- Do not accept pupils (even those that have recently left the school), parents or carers as 'friends'.

- Do not use Facebook or other social networking sites in any way that might bring your professional status or your school into disrepute.

- Taking charge of your digital reputation is important, as unprofessional posts or images will lead to disciplinary action and possible failure to gain employment in the future.

- Do not post or upload photographs relating to colleagues, pupils or parents. Objection to such posts can cause friction in your school and make your working environment uncomfortable.

- Do not post or upload photographs related to school-based or extra-curricular activities and do not make specific reference to your school in any post as comments may be misconstrued and result in inappropriate responses.

- Be aware of any spam or potential virus risks sent via rogue posts. It is advisable to check with anti-virus firms if you get any suspicious requests or posts.

- If you are alerted to any negative or unscrupulous information about yourself, colleagues or your school on Facebook or other social networking sites, inform your headteacher. Further advice to help with cyberbullying incidents etc., can be gained from help@saferinternet.org.uk (0844 3814772) or a professional association such as your Trade Union.

- ***I understand the implications of using Facebook and other social networking sites for my own protection and professional reputation, as well as the impact that my use can have on my school community and establishment.***
- ***I understand that injudicious use of social networking may lead to disciplinary action.***
- ***I agree to take all possible precautions as outlined above.***

Name		***Date***	