Birkdale High School

NIHIL NISI BONUM

Birkdale
High School

Aspire - Thrive - Succeed

eSafety and Data Security Policy

Date of Policy	November 2017
Members of staff responsible	Headteacher (Mr Bourgade)
Review date	November 2019

CONTENTS

Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, Birkdale High School needs to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources, including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile / Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

Here at **Birkdale High School** we understand the responsibility to educate our pupils on eSafety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Birkdale High School holds personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can also result in media coverage, and potentially damage the reputation of Birkdale High School.

Everybody in Birkdale High School has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet technologies provided by Birkdale High School (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc.); and technologies owned by pupils and staff, but brought onto Birkdale High School premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc.).

Monitoring

Authorised ICT staff may inspect any ICT equipment owned or leased by Birkdale High School at any time without prior notice.

ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain Birkdale High School business related information; to confirm or investigate compliance with Birkdale High School policies, standards and procedures; to ensure the effective operation of Birkdale High School ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

ICT authorised staff may, without prior notice, access the e-mail or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Please note that personal communications using Birkdale High School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

The ICT and safeguarding teams perform weekly checks on reported violations. Although it is impossible to check all of them, this process does enable the school to identify false positives, which will make the system more effective over time and identify and resolve potential breaches. A log of all checks is kept by the ICT technician.

Breaches

A breach or suspected breach of policy by a Birkdale High School employee, contractor or pupil may result in the temporary or permanent withdrawal of Birkdale High School ICT hardware, software or services from the offending individual.

Any policy breach is grounds for disciplinary action in accordance with Birkdale High School Disciplinary Procedure.

Policy breaches may also lead to criminal or civil proceedings.

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to Birkdale High School Deputy Headteacher and Line Manager. Additionally, all security breaches, lost / stolen equipment or data (including remote access, Secure ID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to your Line Manager and IT Manager.

Please refer to the relevant section on Incident Reporting, eSafety Incident Log & Infringements.

Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media (e.g. external hard drive, USB pen drive, CD/DVD etc.) will be actively checked for viruses using Birkdale High School's anti-virus measures.

- Never interfere with anti-virus software installed on any Birkdale High School ICT equipment that you use.

- If your school owned portable device is not routinely connected to Birkdale High School network, you must make provision for regular virus updates through the IT Support team.

- If you suspect there may be a virus on any Birkdale High School ICT equipment, stop using the equipment and log a fault with the IT Help Desk. The IT Support Team will carry out any necessary action and the Headteacher will be informed.

Data Security

The accessing and appropriate use of Birkdale High School data is something that Birkdale High School takes very seriously.

Security

- Birkdale High School gives relevant staff access to its Management Information System (SIMS), with a unique username and password.

- It is the responsibility of everyone to keep passwords secure.

- Staff are aware of their responsibility when accessing Birkdale High School data.

- Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use.

- Staff keep all Birkdale High School related data secure. This includes all personal, sensitive, confidential or classified data

- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight

- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under their control at all times

- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when shared copiers (multi-function print, fax, scan and copiers) are used.

Anyone expecting a confidential / sensitive fax, should have warned the sender to notify before it is sent.

Disposal of Redundant ICT Equipment Policy

- All redundant ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data

- All redundant ICT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. We will only use authorised companies who can supply a written guarantee that this will happen.

- Birkdale High School will maintain a comprehensive inventory of all its ICT equipment including a record of disposal

- Birkdale High School’s disposal record will include:

    - Date item disposed of

    - Authorisation for disposal, including:

        - verification of software licensing,

        - any personal data likely to be held on the storage media? *

    - How it was disposed of e.g. waste, gift or sale

    - Name of person and / or organisation who received the disposed item

  ** if personal data is likely to be held, the storage media will be over written multiple times to ensure the data is irretrievably destroyed.*

- Any redundant ICT equipment being considered for sale / gift will be subject to a recent electrical safety check and hold a valid PAT certificate.

E-mail

The use of e-mail within Birkdale High School is an essential means of communication for both staff and pupils. In the context of Birkdale High School, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an e-mail in relation to their age and good network etiquette; ‘netiquette’.

Managing E-mail

- Birkdale High School gives all staff their own e-mail account to use for all Birkdale High School business as a work based tool. This is to minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed

- It is the responsibility of each account holder to keep their password secure. For the safety and security of users and recipients, all e-mail is filtered and logged; if necessary e-mail history can be traced. Staff, governors and pupils should only use their Birkdale High School email account for any Birkdale High School related activities / matters.

- Under no circumstances should staff contact pupils, parents or conduct any Birkdale High School business using personal e-mail addresses

- Birkdale High School requires a standard disclaimer to be attached to all e-mail correspondence which has been setup and maintained by the IT Manager.

- All e-mails should be written and checked carefully before sending, in the same way as a letter written on Birkdale High School headed paper

- Staff sending e-mails to external organisations, parents or pupils are advised to CC. their line manager.

- Staff must inform the Headteacher/Line Manager if they receive an offensive e-mail.

- E-mails sent or received as part of a Birkdale High School role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. Staff must therefore actively manage their e-mail account as follows:

  - Delete all e-mails of short-term value
  - Organise e-mail into folders and carry out frequent house-keeping on all folders and archives

- However staff access their Birkdale High School e-mail (whether directly, through webmail when away from the office or on non-Birkdale High School equipment) all Birkdale High School e-mail policies apply

- The use of Hotmail, BTInternet, AOL or any other Internet based webmail service for sending, reading or receiving business related e-mail is not permitted unless sanctioned by the Headteacher.

- All pupil e-mail users are expected to adhere to the generally accepted rules of netiquette, particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, arranging to meet anyone without specific permission, ensuring files are virus checked before attaching to an e-mail.

- Pupils must immediately tell a teacher / trusted adult if they receive an offensive e-mail.

- Pupils may only use Birkdale High School approved e-mail accounts on Birkdale High School's network, and only under direct teacher supervision for educational purposes.

- Pupils are introduced to e-mail as part of the Year 7 Computing Scheme of Work.

Sending e-Mails

- If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the section titled **E-mailing Personal, Sensitive, Confidential or Classified Information.**

- Use your own Birkdale High School e-mail account so that you are clearly identified as the originator of a message.

- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate.

- Birkdale High School e-mail is not to be used for personal advertising.

Receiving E-mails

- Check your e-mail regularly

- Never open attachments from an untrusted source; consult your IT Manager first.

- Do not use the school e-mail system to store attachments. Detach and save business related work to the appropriate shared drive / folder.

- The automatic forwarding and deletion of e-mails is not allowed

E-mailing Personal, Sensitive, Confidential or Classified Information

- Assess whether the information can be transmitted by other secure means before using e-mail.
- E-mailing confidential data is not recommended and should be avoided where possible.
- The use of Hotmail, BTInternet, AOL or any other Internet based webmail service for sending e-mail containing sensitive information is not permitted.

- Where your conclusion is that e-mail must be used to transmit such data:

  - Obtain express consent from your Line Manager to provide the information by e-mail
  - Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:

    - Verify the details, including accurate e-mail address, of any intended recipient of the information.

  - Verify (by phoning) the details of a requestor before responding to e-mail requests for information.
  - Do not copy or forward the e-mail to any more recipients than is absolutely necessary.

- Do not send the information to anyone whose details you have been unable to separately verify (usually by phone).
- Send the information as an encrypted document **attached** to an e-mail.
- Provide the encryption key or password via a **separate** means of contact with the recipient(s) (e.g. phone).
- Do not identify such information in the subject line of any e-mail.
- Request confirmation of safe receipt.

Equal Opportunities

Pupils with Additional Needs

Staff should be aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues.

Where a pupil has poor social understanding, careful consideration should be given to group interactions when raising awareness of eSafety. Internet activities should be planned carefully and well managed for these children and young people.

eSafety

eSafety - Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within Birkdale High School, the Headteacher and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. eSafety is the responsibility of all staff.

eSafety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for eSafety guidance to be given to the pupils on a regular and meaningful basis. eSafety is embedded within our curriculum and we continually look for new opportunities to promote eSafety.

- Birkdale High School has a framework for teaching internet skills in Computing / PSHE lessons and through pastoral systems

- Birkdale High School provides opportunities within a range of curriculum areas to teach about eSafety

- Educating pupils on the dangers of technologies that maybe encountered outside Birkdale High School is done informally when opportunities arise and as part of the eSafety curriculum

- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them

- Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies;

- During lessons in computer rooms all staff have access to the Impero console that allows remote monitoring of all users' activities in the room.

eSafety Skills Development for Staff

- Our staff receive regular information and training on eSafety issues as part of Birkdale High School's annual safeguarding update.

- New staff receive information on Birkdale High School's acceptable use policy as part of their induction.

- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of eSafety.

- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas

Incident Reporting, eSafety Incident Log & Infringements

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to Birkdale High School's Headteacher and Line Manager.

eSafety Incident Log

Some incidents may need to be recorded in other places, such as the bullying or racist incident logbook or CPOMS.

Misuse and Infringements

Complaints

Complaints and / or issues relating to eSafety should be made to the Headteacher.

Internet Access

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of Birkdale High School's network for internet access is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

Managing the Internet

- Whenever possible staff should preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute Birkdale High School software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

Internet Use

- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended restricted audience. Staff are encouraged to be wary about publishing specific and detailed private thoughts online.
- You must not communicate with any pupil over the internet as Social Media can blur teacher/pupil boundaries.
- Don't reveal names of colleagues, customers or clients or any other confidential information acquired through your job on any social networking site or blog.
- On-line gambling or gaming is not allowed.
- Ensure all your online activity, both in and outside Birkdale High School, will not bring your professional role or Birkdale High School into disrepute.

It is at the Headteacher's discretion on what internet activities are permissible for staff and pupils and how this is disseminated.

Infrastructure

- Birkdale High School also employs some additional web filtering which is the responsibility of the IT Manager (appendix 7). The filtering system blocks sites that fall into categories such as pornography, race hatred, radicalisation, extremism, gaming, social networking and sites of an illegal nature etc. All changes to the filter policy is logged and only available to staff with the approved 'web filtering' management status for teaching.

- Birkdale High School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998

- Staff and pupils are aware that Birkdale High School email and internet activity can be monitored and explored further if required.

- Birkdale High School does not allow pupils access to the internet logs.

- If staff or pupils discover an unsuitable site, the screen must be switched off / closed and the incident reported immediately to the Head of ICT or teacher as appropriate.

- It is the responsibility of Birkdale High School to ensure that anti-virus protection is installed and kept up-to-date on all Birkdale High School workstations.

- Pupils and Staff using personal removable media are responsible for measures to protect against viruses, e.g. making sure that personal systems used have up-to-date anti-virus software. It is not the responsibility of Birkdale High School to install or maintain anti-virus on personal systems.

- Pupils and staff are not permitted to download programs or files on Birkdale High School based technologies without seeking prior permission from the IT Manager.

- If there are any issues related to viruses or anti-virus software, a fault ticket should be logged on the IT Support Desk.

Managing Other Web 2 Technologies

Web 2, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, Birkdale High School endeavours to deny access to social networking sites to pupils and staff within Birkdale High School.

- Staff may only create blogs, wikis or other web 2 spaces in order to communicate with pupils using systems approved by their Line Manager and Headteacher.

- All pupils are advised to be cautious about the information given by others on sites e.g. users not being who they say they are.

- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online

- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile / home phone numbers, Birkdale High School details, IM / email address, specific hobbies / interests)

- Our pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals

- Pupils / staff are encouraged to be wary about publishing specific and detailed private thoughts online.

- Our pupils are asked to report any incidents of cyberbullying to a teacher / trusted adult.

Parental Involvement

We believe that it is essential for parents / carers to be fully involved with promoting eSafety both in and outside of Birkdale High School and also to be aware of their responsibilities. We regularly consult and discuss eSafety with parents / carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- Parents / carers and pupils are encouraged to contribute to adjustments or reviews of Birkdale High School's eSafety policy which is posted on Birkdale High School website.
- Parents / carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to Birkdale High School.
- Parents / carers are required to make a decision as to whether they consent to images of their child being taken / used in the public domain (e.g. on Birkdale High School's website).
- Parents / carers are informed on admission of the Birkdale High School agreement containing the following statement.
    - → **We will support Birkdale High School's approach to on-line safety and not deliberately upload or add any images, sounds or text that could upset or offend any member of the Birkdale High School community.**

Passwords and Password Security

Passwords

- Always use your own usernames and passwords to access computer based services.
- Make sure you enter your username and password each time you logon. Do not include passwords in any automated logon procedures.
- Staff should change temporary passwords at first logon
- Change passwords whenever there is any indication of possible system or password compromise.
- Do not record passwords or encryption keys on paper or in an unprotected file.
- Only disclose your personal password to authorised IT Support staff when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is fulfilled.
- The user accounts belonging to staff and pupils who have left Birkdale High School are disabled. The IT Manager has responsibility for user accounts to be removed from the system and the backup of Home drives in line with the Examination Policy.

If you think your password may have been compromised or someone else has become aware of your password report this to the Head of ICT / IT Manager.

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood Birkdale High School's e-Safety and Data Security Policy.
- Users are provided with an individual network, email, Learning Platform and Management Information System (where appropriate) logon username and password.
- Pupils are not allowed to deliberately access on-line materials or files on Birkdale High School's network belonging to their peers, teachers or others.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of all Birkdale High School systems, including (but not limited to) computer access, remote access, email, SIMS, Learning Platforms and Virtual Learning Environments. Staff must ensure that their passwords are not shared with anyone and are changed periodically. Individual staff users must also make sure that workstations are either locked or logged off when unattended (workstations automatically lock after a set period of time). At the end of each day, workstations that are not in use will automatically shut down at 5pm, followed by a second attempt at 7pm.

Personal or Sensitive Information

Protecting Personal, Sensitive, Confidential and Classified Information

- Ensure that any Birkdale High School information accessed from your own device or removable media equipment is kept secure.

- Ensure you lock the screen before leaving your device unattended, to prevent unauthorised access.

- Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others

- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person

- Ensure the security of any personal, sensitive, confidential and classified information contained in documents you fax, copy, scan or print. This is particularly important when shared devices are used and / or when access is from a non-Birkdale High School environment

- Only download personal data from systems if expressly authorised to do so by your manager

- You must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience

- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information

- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labelling

Storing / Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media

- Ensure removable media purchased for this purpose has an encryption feature.

- Store all removable media securely.

- Securely dispose of removable media that may hold personal data (ask the IT Manager if you need further advice).

- Ensure internal storage devices from equipment no longer in service are removed and stored securely or permanently wiped clean.

- It is the responsibility of staff to encrypt all files containing personal, sensitive, confidential or classified data.

Safe Use of Images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the Birkdale High School community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, Birkdale High School permits the appropriate taking of images by staff and pupils with Birkdale High School equipment.

- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils. This includes when on field trips. However, with the express permission of the Headteacher, images can be taken provided they are transferred immediately to Birkdale High School's network or Birkdale's branded social media and deleted from the staff device.

- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of others. This includes when on field trips. However, with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to Birkdale High School's network and deleted from the pupil's device

Consent of Adults Who Work at Birkdale High School

- Permission to use images of all staff who work at Birkdale High School is sought on induction and a copy is located in their personnel files.

Publishing Pupil's Images and Work

On a child's entry to Birkdale High School, all parents / carers will be asked to give permission to use their child's work / photos in the following ways:

- on the Birkdale High School web site,

- on Birkdale High School's social media platforms,

- in Birkdale High School's prospectus and other printed publications that Birkdale High School may produce for promotional purposes,

- recorded / transmitted by audio, video or webcam,

- in display material that may be used in Birkdale High School's communal areas,

- in display material that may be used in external areas, i.e. exhibition promoting Birkdale High School,

- general media appearances, e.g. local / national media / press releases sent to the press highlighting an activity (sent using traditional methods or electronically).

This consent form is considered valid for the entire period that the child attends Birkdale High School, unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

Parents / carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.

Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.

Before posting pupils' work on the Internet, a check with the school office needs to be made to ensure that permission has been given for that particular work to be displayed.

Storage of Images

- Images / films of children are stored on Birkdale High School's network
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g. USB pen drives, personal mobile phones) without the express permission of the Headteacher.
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of Birkdale High School's network.
- Arrangements will be made with the IT Manager to ensure the deletion of images when they are no longer required, or after the pupil has left Birkdale High School.

Webcams and CCTV – (please see Birkdale High School's CCTV Policy)

- Birkdale High School uses CCTV for security and safety. This is managed by the Site Manager / IT Manager. Notification of CCTV usage is displayed at the front of Birkdale High School.
- Webcams in Birkdale High School should only ever be used for specific learning purposes (e.g. monitoring of the school pond) and never used to record/broadcast images of children or adults.
- Misuse of a webcam by any member of the Birkdale High School community will result in sanctions and may lead to disciplinary action in accordance with Birkdale High School procedures.
- Consent is sought from parents / carers and staff when joining Birkdale High School, in the same way consent is sought for all types of images used for school purposes.

Video Conferencing

- Permission is sought from parents / carers if their children are involved in video conferences with end-points outside of Birkdale High School.
- All pupils should be supervised by a member of staff when video conferencing.

ICT Equipment, Portable & Mobile Including Removable Media

Birkdale High School ICT Equipment

- As a user of ICT, you are responsible for any activity undertaken on Birkdale High School's ICT equipment provided to you.

- Personal or sensitive data should not be stored on the local drives of workstations. If it is necessary to do so, the local drive must be encrypted.

- Workstations that are connected to the school domain have an auto lock policy (45 minutes) which is applied to all staff users. If a member of staff has a school device which does not rely on the network to function correctly (standalone) such as a laptop or tablet, it must have an auto lock feature enabled.

- Privately owned ICT equipment should not be used on any Birkdale High School network, unless connected through the BYOD network.

- On termination of employment, resignation or transfer, return all ICT equipment to your Line Manager. You must also provide details of all your system logons so that they can be disabled.

- It is your responsibility to ensure that any information accessed from your own workstation or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person.

Portable & Mobile ICT Equipment

This section covers portable devices, such as laptops, tablets, PDAs and removable data storage etc. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data.

- All activities carried out on Birkdale High School systems and equipment will be monitored in accordance with this policy.

- Staff must ensure that all Birkdale High School data is stored on Birkdale High School's network, and not kept locally on a portable device. If this is unavoidable, any data stored on a portable device must be encrypted.

- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey

- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight

- Portable equipment must be transported in its protective case if supplied

Servers

- All Birkdale High School servers are in a locked and secure environment.
- Strict access rights are enforced in this area.
- All severs are password protected.
- All servers have security software installed appropriate to the machine's specification.
- A full backup of all servers is performed each week, with incremental backups on the days in-between. All backups are stored in a separate building which is also secure.

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, tablets, gaming devices, mobile and smart phones are familiar to children outside of Birkdale High School too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in Birkdale High School is allowed. Birkdale High School chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile Devices (including phones)

- Birkdale High School allows staff to bring in personal mobile phones and devices for their own use. Members of staff should only contact a parent/carer using their personal device in exceptional circumstances, barring their number. Contacting a pupil should only be done with express authorisation from the Headteacher.
- Under no circumstances should a member of staff put themselves at risk by having contact details, data or photographs of any student stored on their personal device (any necessary contact should be via school / pool mobiles). This will lead to disciplinary action in accordance with Birkdale High School procedures
- Pupils are allowed to bring their own mobile phone to Birkdale High School, but it cannot be used for personal reasons within lesson time. At all times their device must be switched to silent mode and only used in designated areas.
- Pupils personal mobile devices (tablet, laptop etc.) may be used, however, for educational purposes, as mutually agreed with the teacher. The user, in this instance, must have prior permission from the owner/ bill payer before using their device for this purpose.
- Birkdale High School is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages / electronic communication between any members of the Birkdale High School community is not allowed.
- Users bringing personal devices into Birkdale High School must ensure there is no inappropriate or illegal content on the device.

Staff Responsibilities - Systems and Access

Responsibilities when using any form of ICT, including the Internet, in school and outside of school:

- You are responsible for all activity on Birkdale High School systems carried out under any access / account rights assigned to you, whether accessed via Birkdale High School ICT equipment or your own device.

- Do not allow any unauthorised person to use Birkdale High School ICT facilities and services that have been provided to you.

- Use only your own personal logons, account IDs and passwords and do not allow them to be used by anyone else.

- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information.

- Ensure you lock the screen of your workstation / device before leaving it unattended - to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access.

- Ensure that you logoff from the workstation completely when you are going to be away from for a longer period of time.

- Do not introduce or propagate viruses

- It is imperative that you do not access, load, store, post or send from Birkdale High School systems any material that is, or may be considered to be, illegal, offensive, libellous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to Birkdale High School or may bring Birkdale High School into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of Birkdale High School's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act).

- Any information held on Birkdale High School systems / equipment, or used in relation to Birkdale High School business, may be subject to The Freedom of Information Act.

- Where necessary, obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998.

- It is essential that any storage devices which may have held personal or confidential data are 'scrubbed' in way that means the data can no longer be read. It is not sufficient to simply delete the files or reformat the hard drive. Whoever you appoint to dispose of the equipment must provide a **written guarantee** that they will irretrievably destroy the data by multiple over writing the data.

Social Media (Facebook, Twitter, Instagram etc.)

Facebook, Twitter and other forms of social media are increasingly becoming an important part of our daily lives.

- Our school uses Facebook and Twitter to communicate with parents and carers. The Headteacher my delegate responsibility for all postings on these technologies and will monitor responses from others as well as posts.

- Staff are **not permitted** to access their personal social media accounts using school equipment at any time.

- Staff are able to setup Social Learning Platform accounts, using their school email address, in order to be able to teach pupils the safe and responsible use of Social Media.

- Pupils are **not permitted** to access their social media accounts whilst at school.

- Staff, governors, pupils, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others.

- Staff, governors, pupils, parents and carers are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever.

- Staff, governors, pupils, parents and carers are aware that their online behaviour should at all times be compatible with UK law.

Staff are made aware that social media can blur boundaries. Pupils may see messages / images posted by staff on social media, which could lead to a change in perception of those staff and the school as a whole. A recurring theme of serious incidents over the years shows staff having over-familiar relationships with students, and social media increases this risk.

Here at Birkdale High School we have a strong culture of professional pupil / teacher relationships, and a strong safeguarding policy that has absolute clarity on:

- staff should not befriend students on any social media (this applies to all students under the age of 18).

- staff should be careful when posting on any social media (see staff code of conduct policy).

A breach of these points would result in disciplinary investigation and may result a disciplinary action.

Telephone Services

- You may make or receive personal telephone calls provided:

    1. they are infrequent, kept as brief as possible and do not cause annoyance to others,

    2. they are not for profit or to premium rate services,

    3. they conform to this and other relevant Birkdale High School policies.

- Birkdale High School telephones are provided specifically for Birkdale High School business purposes and personal usage is a privilege that will be withdrawn if abused.

- Be aware that the laws of slander apply to telephone calls. Whilst a telephone call may seem to have a temporary and private existence it still qualifies as admissible evidence in slander law cases.

- Ensure that your incoming telephone calls can be handled at all times.

APPENDICES

Birkdale High School
Acceptable Use of ICT Agreement for Staff

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in Birkdale High School. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Mr G. Bourgade (Headteacher).

1. I will only use Birkdale High School's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Headteacher or Governing Body.
2. I will comply with the ICT system security and not disclose any passwords provided to me by Birkdale High School or other related authorities
3. I will ensure that all electronic communications with pupils and staff are compatible with my professional role and are carried out with Birkdale High school equipment.
4. I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils or parents.
5. I will only use the approved, secure e-mail system(s) for any Birkdale High School business.
6. I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in Birkdale High School, taken off Birkdale High School premises or accessed remotely. Personal data can only be taken out of Birkdale High School or accessed remotely when authorised by the Headteacher or Governing Body. Personal or sensitive data taken off site must be encrypted.
7. I will not install any hardware of software without permission of the IT Manager.
8. I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
9. Images of pupils and / or staff will only be taken, stored and used for professional purposes in line with Birkdale High School policy and with written consent of the applicable parent, carer or staff member. Images will not be distributed outside Birkdale High School's network without the permission of the applicable parent / carer, member of staff or Headteacher.
10. I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
11. I understand that any files / messages stored on Birkdale High School's systems / devices may be removed if deemed inappropriate.
12. I will support Birkdale High School approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the Birkdale High School community.
13. I will respect copyright and intellectual property rights.
14. I will ensure that my online activity, both in and outside Birkdale High School, will not bring my professional role or Birkdale High School into disrepute.
15. I will support and promote Birkdale High School's e-Safety and Data Security Policy and help pupils to be safe and responsible in their use of ICT and related technologies.
16. I understand that it is my professional duty to read Birkdale High School's eSafety and Data Security Policy and comply with the guidance contained therein.
17. I understand this forms part of the terms and conditions set out in my contract of employment.

Staff Signature
I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school.

Staff Signature ______________________ Date ______________

Printed Full Name ______________________ Job Title ______________

Birkdale High School
Acceptable Use of ICT Agreement for Governors
(Includes guest network access)

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This document is designed to ensure that all governors are aware of their responsibilities when using any form of ICT. All governors are expected to sign this document. Further guidance can be found in the school's eSafety and Data Security Policy.

1. I will only use the School's e-mail / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Headteacher or Governing Body.
2. I will comply with the ICT system security and not disclose any passwords provided to me by Birkdale High School or other related authorities
3. I will ensure that all electronic communications with pupils and staff are professional and compatible with my role.
4. I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils or parents.
5. I will not install any hardware of software without permission of the IT Manager.
6. I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
7. Images of pupils and / or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the applicable parent, carer or staff member. Images will not be distributed outside Birkdale High School's network without the permission of the applicable parent / carer, member of staff or Headteacher.
8. I understand that all my use of the Internet and other related technologies on the school network can be monitored and logged and can be made available, on request, to the Headteacher.
9. I understand that any files / messages stored on Birkdale High School's systems / devices may be removed if deemed inappropriate.
10. I will support Birkdale High School's approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the Birkdale High School community.
11. I will respect copyright and intellectual property rights.
12. I will ensure that my online activity, both in and outside Birkdale High School, will not bring my role or the school into disrepute.
13. I will support and promote Birkdale High School's e-Safety and Data Security Policy and help pupils to be safe and responsible in their use of ICT and related technologies.
14. I will take every precaution to ensure that all electronic communications related to my role as a governor are kept secure and treated as confidential.
15. I understand that I have a duty to report any incidents or concerns regarding e-Safety to the Deputy Headteacher / Headteacher.
16. I understand that if using the school network, it is my duty to read Birkdale High School's eSafety and Data Security Policy and comply with the guidance contained therein.

Governor Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school.

Governor Signature ______________________ Date ______________

Printed Full Name ______________________ Job Title ______________

Birkdale High School
Acceptable Use of ICT Agreement for Visitors
(With guest network access)

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This document is designed to ensure that all visitors are aware of their responsibilities when using any form of ICT. All visitors are expected to sign this document. Further guidance can be found in the school's eSafety and Data Security Policy.

1. I will only use Birkdale High School's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Headteacher or Governing Body.
2. I will comply with the ICT system security and not disclose any passwords provided to me by Birkdale High School or other related authorities.
3. I will ensure that all electronic communications with pupils and staff are professional and compatible with my role.
4. I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils and parents.
5. I will not install any hardware of software without permission of the IT Manager.
6. I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
7. Images of pupils and / or staff will only be taken, stored and used for professional purposes in line with Birkdale High School policy and with written consent of the applicable parent, carer or staff member. Images will not be distributed outside the school network without the permission of the applicable parent / carer, member of staff or Headteacher.
8. I understand that all my use of the Internet and other related technologies on the school network can be monitored and logged and can be made available, on request, to the Head teacher.
9. I understand that any files / messages stored on Birkdale High School's systems / devices may be removed if deemed inappropriate.
10. I will support Birkdale High School's approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the School community
11. I will respect copyright and intellectual property rights.
12. I will ensure that my online activity, both in and outside Birkdale High School, will not bring my role or the school into disrepute.
13. I will support and promote the Birkdale High School's e-Safety and Data Security Policy and help pupils to be safe and responsible in their use of ICT and related technologies.
14. I will take every precaution to ensure that all electronic communications related to my role are kept secure and treated as confidential.
15. I understand that I have a duty to report any incidents or concerns regarding e-Safety to the Deputy Headteacher / Headteacher.
16. I understand that if using the school network, it is my duty to read the Birkdale High School eSafety and Data Security Policy and comply with the guidance contained therein.

Visitor Signature
I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school.

Visitor Signature ______________________ Date ______________________

Printed Full Name ______________________ Job Title ______________________

Birkdale High School Academy

Acceptable Computer & Internet Use Policy for Students

The School Network (which includes all computers, laptops, tablets, e-mail and Internet access) is owned by the School and is made available to pupils to enhance their own learning. The School's Acceptable Use Policy has been drawn up to protect all parties – the pupils, staff and the School.

When students are allowed to use computers or the Internet, they will be expected to follow these rules:

While using computers, laptops, tablets, email or the Internet at Birkdale High School Academy

1. I will remember that the school has an ethos of Respect and Service and ensure that I carry it out.
2. I will only use the computer for educational activities.
3. I will not use any computer in such a way that would disrupt the computer use of others.
4. I will not attempt to access, edit or delete files or areas belonging to others.
5. I will not interfere with any computer security measures the school may have in place or attempt to bypass the internet filtering system.
6. I will not use someone else's username and password to access the computer system, even if they have given me permission to do so.
7. I will not give anyone else my username and password.
8. I will not reveal personal details, address, phone number or password of others, or myself.
9. I will only upload, download or copy files to, or from, the internet with the permission of a member of staff.
10. I will respect copyright and intellectual property rights
11. I will only use the school printing facilities for printing academic work.
12. I will not attempt to access or download files from the internet or install software unless instructed to do so by a member of staff.
13. I will ensure that my online activity, both in school and outside school, will not cause others distress or bring the school, its staff or pupils into disrepute.
14. I will not use bad language, flaming or insight bullying in any messages I send.
15. I will not try to visit sites which might have offensive material.
16. I will report any unpleasant material or messages sent to me. I understand my report will be confidential and would help protect other pupils and myself.
17. I will not access chatrooms, instant messaging, social networking sites or other online email services
18. Images of pupils and / or staff will only be taken, stored and used for school purposes in line with school policy and not be distributed outside the school network without the permission of a member of staff.

17. Users should be aware that monitoring and random checks are made on all computer use and all e-mail messages sent and received, and that records are kept. I understand that any files / messages stored on Birkdale High School's systems / devices may be removed if deemed inappropriate.

All rules relating to computer use apply to both computer networks and stand-alone devices in the school. These rules also apply to all information sent electronically within the school, including text messages or pictures sent by mobile phones.

Should any pupil feel upset by either an e-mail or text message in school they can e-mail dpryor@birkdalehigh.co.uk where their concerns will be dealt with in confidence.

Birkdale High School Academy

Acceptable Computer & Internet Use Policy for Students

PARENT/GUARDIAN

As the parent or guardian of ____ Form:

I have read the rules for Acceptable Computer and Internet Use and understand that these rules apply when my child is using school computers and the Internet, and all information sent electronically within school.

I have gone through the rules with my child and explained their importance and the consequences of breaking the rules.

I understand that

- Computers and Internet access at Birkdale High School Academy are provided for educational purposes only.
- Birkdale High School will follow all educational guidelines on protecting students from unsuitable material.
- The school will make every reasonable effort to restrict access to all controversial material on the Internet, but I will not hold them responsible for materials my child acquires or sees as a result of the use of the Internet at school.

I give my permission to Birkdale High School Academy to allow the student named above to use the computers and Internet in the school. (This can be changed at any time, just contact your child's Head of Year.)

Parent's signature ____

Date ____

The school will provide your child with an e-mail address for use in school. All e-mail entering and leaving the school is checked for viruses, offensive content and SPAM. The IT Department will also monitor use of e-mail and conduct random checks to ensure that e-mail is being used appropriately.

I give my permission to Birkdale High School Academy to allow the student named above to use the school's e-mail system. (This can be changed at any time, just contact your child's Head of Year.)

Parent's signature ____

Date ____

STUDENT

I have read the rules for Acceptable Computer and Internet Use and know the importance of these rules.

I know that if I break these rules, I might lose the right to use the school's computer facilities or face further disciplinary action.

Student's signature ____

Date ____

Birkdale High School Academy

Pupil & parent consent for the use of images

Use of photographic images of pupils by parents

As the child's parents / carers, we agree that if we take photographs or video recordings of our children which include other students, we will use these for personal and family use only. I / We understand that where consent has not been obtained from the other parents for any other use, we would be in breach of the Data Protection Act 1998 if we used our recordings for any wider purpose.

Signature of parent/carer________________________ Date__________________

Use of photographic images of pupils by school

There may be occasions during the year when your child may be photographed or filmed during school activities in accordance with school policy (see attached). **Only tick the box below and sign this section if you do not wish your child to be photographed or filmed, and return this form to the school office. If you agree, please leave blank.**

□ I **do not** wish my child _________________________ to be photographed or filmed during school activities **at any time**. This will include all school, group and class photos and any special event.

□ I **do not** wish for any work produced by my child _________________________ to be published, used or displayed in any form (website or school learning platform, prospectus, internal or external displays or for use by local or national media).

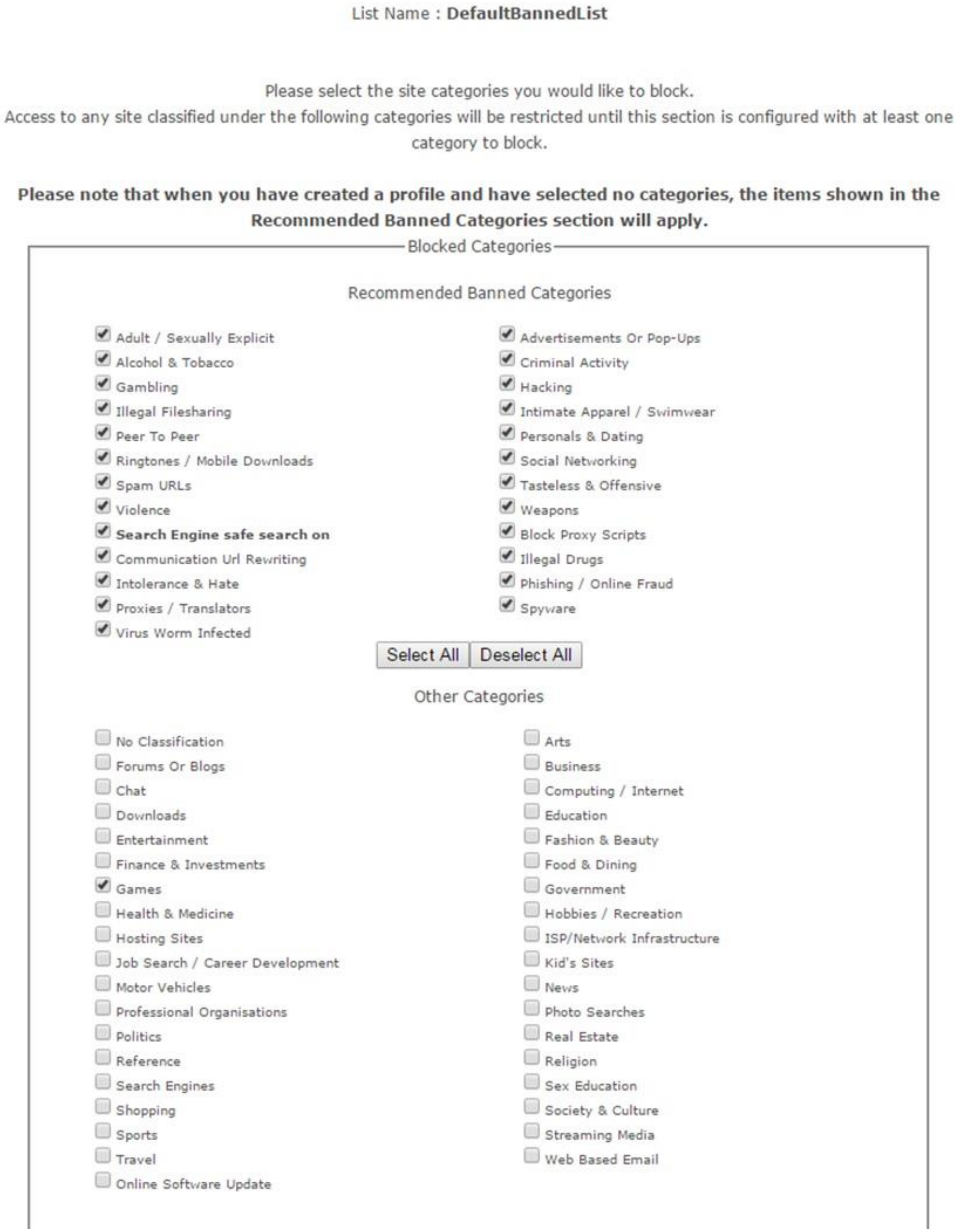
Signature of parent/carer________________________ Date__________________

This form is valid from the date you sign it, for the period of time your child attends this school. The consent will automatically expire after this time. It is your responsibility to let us know if you want to withdraw or change your agreement at any time.

IT Support Operating Hours

Weekday	Start Time	Finish Time
Monday	08:00	16:45
Tuesday	08:00	16:45
Wednesday	08:00	16:45
Thursday	08:00	16:45
Friday	08:00	16:00

SurfProtect (Internet Filtering)



List Name : **DefaultBannedList**

Please select the site categories you would like to block.
Access to any site classified under the following categories will be restricted until this section is configured with at least one category to block.

Please note that when you have created a profile and have selected no categories, the items shown in the Recommended Banned Categories section will apply.

Blocked Categories

Recommended Banned Categories

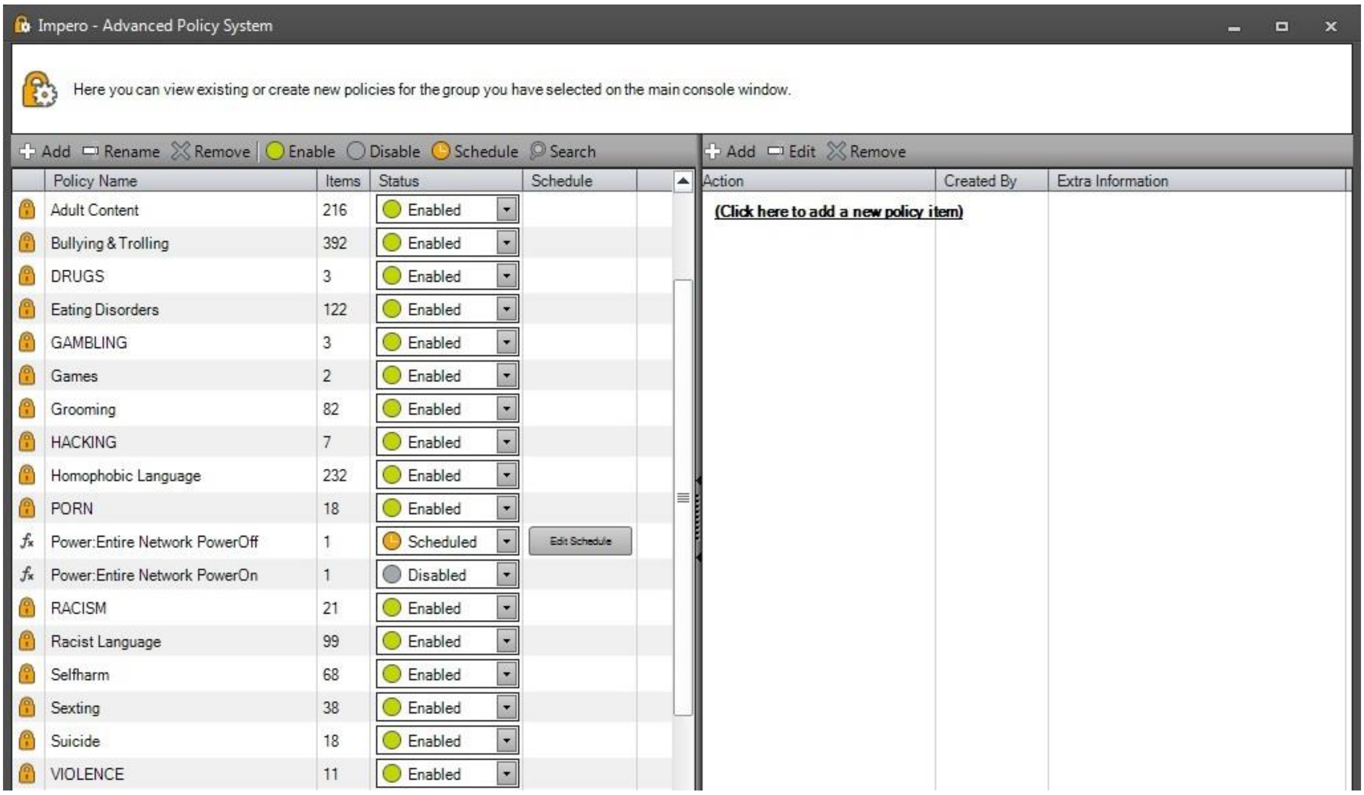
- ☑ Adult / Sexually Explicit
- ☑ Alcohol & Tobacco
- ☑ Gambling
- ☑ Illegal Filesharing
- ☑ Peer To Peer
- ☑ Ringtones / Mobile Downloads
- ☑ Spam URLs
- ☑ Violence
- ☑ **Search Engine safe search on**
- ☑ Communication Url Rewriting
- ☑ Intolerance & Hate
- ☑ Proxies / Translators
- ☑ Virus Worm Infected
- ☑ Advertisements Or Pop-Ups
- ☑ Criminal Activity
- ☑ Hacking
- ☑ Intimate Apparel / Swimwear
- ☑ Personals & Dating
- ☑ Social Networking
- ☑ Tasteless & Offensive
- ☑ Weapons
- ☑ Block Proxy Scripts
- ☑ Illegal Drugs
- ☑ Phishing / Online Fraud
- ☑ Spyware

Select All | Deselect All

Other Categories

- □ No Classification
- □ Forums Or Blogs
- □ Chat
- □ Downloads
- □ Entertainment
- □ Finance & Investments
- ☑ Games
- □ Health & Medicine
- □ Hosting Sites
- □ Job Search / Career Development
- □ Motor Vehicles
- □ Professional Organisations
- □ Politics
- □ Reference
- □ Search Engines
- □ Shopping
- □ Sports
- □ Travel
- □ Online Software Update
- □ Arts
- □ Business
- □ Computing / Internet
- □ Education
- □ Fashion & Beauty
- □ Food & Dining
- □ Government
- □ Hobbies / Recreation
- □ ISP/Network Infrastructure
- □ Kid's Sites
- □ News
- □ Photo Searches
- □ Real Estate
- □ Religion
- □ Sex Education
- □ Society & Culture
- □ Streaming Media
- □ Web Based Email

Impero (Internet Filtering)



Here you can view existing or create new policies for the group you have selected on the main console window.

Policy Name	Items	Status	Schedule
Adult Content	216	Enabled	
Bullying & Trolling	392	Enabled	
DRUGS	3	Enabled	
Eating Disorders	122	Enabled	
GAMBLING	3	Enabled	
Games	2	Enabled	
Grooming	82	Enabled	
HACKING	7	Enabled	
Homophobic Language	232	Enabled	
PORN	18	Enabled	
Power:Entire Network PowerOff	1	Scheduled	Edit Schedule
Power:Entire Network PowerOn	1	Disabled	
RACISM	21	Enabled	
Racist Language	99	Enabled	
Selfharm	68	Enabled	
Sexting	38	Enabled	
Suicide	18	Enabled	
VIOLENCE	11	Enabled	

Action	Created By	Extra Information
(Click here to add a new policy item)		