Birkdale High School

Data Security Policy

November 2020-21

NIHIL NISI BONUM

Birkdale
High School

Aspire - Thrive - Succeed

Birkdale High School
Data Security Policy

Date of Policy: *November 2020*
Members of staff responsible: *Headteacher*
Review date: *November 2021*

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
- Email 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 2018, 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 and GDPR 2018.

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.

Internet usage is monitored and logged, reports are generated on a daily basis for those triggering multiple hits in categories Mental Health, Threats to Harm, High Risk and Productivity Loss.

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 email 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 Deputy 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, 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 overwritten multiple times or encrypted 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.

Email

The use of email within Birkdale High School is an essential means of communication for both staff and pupils. In the context of Birkdale High School, email should not be considered private. Educationally, email 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 email in relation to their age and good network etiquette; 'netiquette'. In order to achieve ICT level 4 or above, pupils must have experienced sending and receiving emails, which is taught in Year 7.

Managing Email

- Birkdale High School gives all staff their own email 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 emails 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 email is filtered and logged; if necessary email 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 email addresses
- Birkdale High School requires a standard disclaimer to be attached to all email correspondence which has been setup and maintained by the IT Manager.
- All emails should be written and checked carefully before sending, in the same way as a letter written on Birkdale High School headed paper
- Staff sending emails to external organisations, parents or pupils are advised to CC. their line manager.
- Staff must inform the Deputy Headteacher / Line Manager if they receive an offensive email.
- Emails sent or received as part of your Birkdale High School role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your email account as follows:
    - Delete all emails of short-term value
    - Organise email into folders and carry out frequent house-keeping on all folders and archives
- However you access your Birkdale High School email (whether directly, through webmail when away from the office or on non-Birkdale High School equipment) all Birkdale High School email policies apply
- The use of Hotmail, BTInternet, AOL or any other Internet based webmail service for sending, reading or receiving business related email is not permitted unless sanctioned by the Headteacher.
- All pupil email 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 email communication, arranging to meet anyone without specific permission, ensuring files are virus checked before attaching to an email.
- Pupils must immediately tell a teacher / trusted adult if they receive an offensive email.
- Pupils may only use Birkdale High School approved email accounts on Birkdale High School's network, and only under direct teacher supervision for educational purposes.
- Pupils are introduced to email as part of the Year 7 Computing Scheme of Work.

Sending Emails

- If sending emails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the section titled **Emailing Personal, Sensitive, Confidential or Classified Information.**
- Use your own Birkdale High School email account so that you are clearly identified as the originator of a message.

- Keep the number and relevance of email recipients, particularly those being copied, to the minimum necessary and appropriate.
- Birkdale High School email is not to be used for personal advertising.

Receiving Emails

- Check your email regularly
- Never open attachments from an untrusted source; consult your IT Manager first.
- Do not use the school email system to store attachments. Detach and save business related work to the appropriate shared drive / folder.
- The automatic forwarding and deletion of emails is not allowed

Emailing Personal, Sensitive, Confidential or Classified Information

- Assess whether the information can be transmitted by other secure means before using email.
- Emailing 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 email containing sensitive information is not permitted.
- Where your conclusion is that email must be used to transmit such data:
- Obtain express consent from your Line Manager to provide the information by email
- Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:
    - Verify the details, including accurate email address, of any intended recipient of the information.
    - Verify (by phoning) the details of a requestor before responding to email requests for information.
    - Do not copy or forward the email 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 email.
- 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 email.
- Request confirmation of safe receipt.

E-mail Retention

Please see Birkdale High School Data Retention Policy.

Passwords and Password Security

Passwords

- Always use your own usernames and passwords to access computer based services.
- 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 IT Support team.

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 Policies.
- 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 online 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 and solely to Birkdale High School's network 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 website,
- on Birkdale High School's Learning 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.

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 (20 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 servers 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 smartphones 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. Under no circumstances does Birkdale High School allow a member of staff to contact a pupil or parent / carer using their personal device
- 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 log off from the workstation completely when you are going to be away 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 a 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 overwriting 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.

- Social Media account holders responsible for all postings on these technologies and monitors responses from others regarding their posts.
- Staff are **not permitted** to access their personal social media accounts using school equipment at any time.
- Staff are able to set up 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 in a disciplinary action.