



Westmorland  
School

# **Data Protection Policy**

**(inc BYOD Guidance)**

**Last Update: October 2021**

**Next Update: September 2022**

Witherslack Group Data Protection Policy		
Date reviewed	Reviewer	Notes
09/08/18	K Spedding	Updated to further reflect DPA 2018 and GDPR.
28/08/2019	K Spedding	Annual review of policy - updated
17/07/20	K Spedding	Annual review of policy – no updates required
21/07/21	K Spedding	Annual review of policy – footer amended, subject access updated
19/10/2021	K Spedding	Section 4. c updated to reflect authority required to take personal data home for work purposes

**Data Protection Policy**

1. **Scope of the Policy:**
2. **The Witherslack Group Will:**
3. **Our Privacy Notices:**
4. **Responsibilities**
5. **Requesting Data (Subject Access Request)**
6. **Security of Personal Data**
7. **Breaches of Personal Data**

**1. Scope of the Policy:**

The Witherslack Group (We, Us, Our) believe that protecting the privacy of our staff and children/young people and regulating their safety through data management, control, and evaluation is vital to whole-establishment and individual progress.

We collect personal data from children/young people, parents/carers, and staff and process it in order to support safeguarding, teaching, learning, monitoring and reporting on child/young person and staff progress, and to strengthen our pastoral provision.

More specific detail on what information is collated, why it is collated, how it is used, shared and secured can be obtained in the Witherslack Group Privacy Notice. We are registered with the ICO ref number Z3410582.

We take responsibility for ensuring that any data that We collect and process is used correctly and only as is necessary. The establishment will keep all affected parties fully informed of how data is collected, what is collected, and how it is used. National curriculum results, attendance and registration records, special educational needs data, and any relevant medical information are examples of the type of data that We need. Through effective data management we can monitor the full range of Our provisions allowing Us to evaluate the wellbeing and academic progression of Our Group to ensure that we are doing all that we can to support both staff and children/young people.

The purpose of this policy is to ensure that all staff and young people within the Group comply with the provisions of the current Data Protection Legislation including Data Protection Act 2018 and (UK) General Data Protection Regulations 2016.

## **2. The Witherslack Group will:**

In line with the current Data Protection Legislation including Data Protection Act 2018 and (UK) General Data Protection Regulations 2016. We will adhere to the requirements of Article 5: principles relating to the processing of personal data.

**Personal Data** is described as;

- Personal data is information that relates to an identified or identifiable individual.
- What identifies an individual could be as simple as a name or a number or could include other identifiers such as an IP address or a cookie identifier, or other factors.
- If it is possible to identify an individual directly from the information you are processing, then that information may be personal data.
- If you cannot directly identify an individual from that information, then you need to consider whether the individual is still identifiable. You should take into account the information you are processing together with all the means reasonably likely to be used by either you or any other person to identify that individual.
- Even if an individual is identified or identifiable, directly or indirectly, from the data you are processing, it is not personal data unless it 'relates to' the individual.
- When considering whether information 'relates to' an individual, you need to take into account a range of factors, including the content of the information, the purpose or purposes for which you are processing it and the likely impact or effect of that processing on the individual.

**Personal Data Shall be :**

- a) Processed lawfully, fairly and in a transparent manner in relation to individuals;
- b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- f) Processed in a manner which ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

In line with the current Data Protection Legislation including Data Protection Act 2018 and (UK) General Data Protection Regulations 2016., We will adhere to the requirements of Article 6 ensuring We have:

- (a) **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.
- (b) **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into contract.
- (c) **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).
- (d) **Vital interests:** the processing is necessary to protect someone's life.
- (e) **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- (f) **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks).

Where the data being processed is categorised as special category data this may create more significant risks to a person's fundamental rights and freedoms and may potentially place them at risk.

When processing data of this nature and in line with the current Data Protection Legislation including Data Protection Act 2018 and (UK) General Data Protection Regulations 2016, the establishment will adhere to the requirements of Article 9 (2) We will ensure that;

- (a) The data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
- (b) Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
- (c) Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- (d) Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
- (e) Processing relates to personal data which are manifestly made public by the data subject;
- (f) Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- (g) Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to

safeguard the fundamental rights and the interests of the data subject;

- (h) Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
- (i) Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or (domestic) Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
- (j) Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or (domestic) Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

There may be circumstances where we are required either by law or in the best interests of our child/young persons or staff to pass information onto external authorities, for example:

- Our local authorities, *statutory regulation as placing authorities and safeguarding*;
- Ofsted, *statutory regulation to help govern and monitor educational system*;
- The Department of Health, *statutory regulation to maintain health*;
- Examination Authorities, *qualification registrations*;
- Police and Courts *statutory obligation to prevent detect crime*.

These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect. They will be data Controllers in their own right and where appropriate will have joint controller agreements.

Under no circumstances will We disclose information or data:

- That would cause serious harm to the child/young person or anyone else's physical or mental health or condition.
- Indicating that the child/young person is or has been subject to child abuse or may be at risk of it, where the disclosure would not be in the best interests of the child/young person recorded by the child/young person in an examination.
- That would allow another person to be identified or identifies another person as the source, unless the person is an employee of the establishment or the Witherslack Group or has given consent, or it is reasonable in the circumstances to disclose the information without consent. The exemption from disclosure does not apply if the information can be edited so that the person's name or identifying details are removed.
- In the form of a confidential reference given to another establishment or any other place of education and training, the child/young person's potential employer, or any national body concerned with child/young person admissions.

### **3. Our Privacy Notice:**

Our external Privacy Notice is split into 5 headings

- Contact Privacy Notice
- Staff Privacy Notice
- Young People Privacy Notice
- Registration for recruitment
- Job Applicant

The Privacy Notice provides more detail on;

- Who are We
- Why We collect and use information
- How We store your information (and for how long)
- Who do We share your information with
- Why do We share your information
- Your rights in relation to your information

The Privacy Notice is available through the link at the bottom of the web page -

[www.witherslackgroup.co.uk](http://www.witherslackgroup.co.uk)

Where appropriate we hold additional privacy notices for specific business areas with which you may engage.

#### **4. Responsibilities:**

##### **[a] The Witherslack Group responsibilities**

We will implement appropriate technical and organisational measures which ensure and demonstrate that We comply with the current Data Protection Legislation including Data Protection Act 2018 and (UK) General Data Protection Regulations 2016. This includes internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal HR policies;

We have appointed a Data Protection officer who will:

- assist to monitor internal compliance;
- inform and advise on Our data protection obligations;
- provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority;
- act as a contact point for the ICO;
- co-operate with the ICO, including during prior consultations under Article 36, and will consult on any other matter;
- implement measures that meet the principles of data protection by design and data protection by default. Measures will include but are not limited to consideration of:
  - data minimisation;
  - pseudonymisation;
  - transparency;
  - allowing individuals to monitor processing; and
  - creating and improving security features on an on-going basis;
  - use of data protection impact assessments.

- be easily accessible as a point of contact for our employees, individuals and the ICO.

#### **[b] Data Protection Team responsibilities**

The Data Protection Team holds responsibility for:

- Drawing up guidance, giving advice and promoting compliance with this policy in such a way as to ensure the easy, appropriate and timely retrieval of information;
- The appropriate compliance with subject access rights and ensuring that data is released in accordance with subject access legislation under the current Data Protection Legislation including Data Protection Act 2018 and (UK) General Data Protection Regulations 2016;
- Ensuring that any data protection breaches are investigated, resolved, catalogued and reported appropriately in a swift manner and in line with guidance from the Information Commissioner's Office;
- Investigating and responding to complaints regarding data protection including requests to rectify and to cease processing personal data.

#### **[c] Staff responsibilities**

Staff members who process personal data about young people, staff, applicants, referrals or any other individual must comply with the requirements of this policy.

Staff members must ensure that:

- All personal data is kept securely; Data, records, and personal information should be stored out of sight and in a locked cupboard no matter what format it is in. The only exception to this is medical information that may require immediate access during the working day. This will be stored securely in an appropriately accessible place. (see clear desk and screen policy)
- Any personal data or hardware/file containing that data that cannot be accounted for due to the fact it is lost or stolen (e.g. Phone laptop, usb, files) must be immediately reported to the Data Protection team as outlined in para 7 of this policy.
- Sensitive or personal information and data should ideally not be removed from the establishment site, however the establishment acknowledges that some staff may need to transport data between the establishment and their home in order to access it for work in the evenings and at weekends. This may also apply in cases where staff have offsite meetings, or are on establishment visits with children/young people. In all cases this must be authorised in writing (including by email) by a manager.
- In accordance with the IT Systems and Services Acceptable Use Policy No Witherslack group Personal Data is to be emailed to a staff members personal account and where personal data is emailed to a third party, external to the Witherslack Group, it must be sent encrypted.
- Any data protection breaches are **immediately** brought to the attention of the Data Protection Team and that staff members support the Data Protection Team in resolving breaches. A breach response plan providing advice and forms is available on the intranet.

The following guidelines are in place for staff in order to reduce the risk of personal data being compromised:

- Paper copies of data or personal information should not be taken off the establishment site. If these are misplaced they are easily accessed. If there is no way to avoid taking a paper copy of data off the establishment site, the information should not be on view in public places, or left unattended under any circumstances.
- Unwanted paper copies of data, sensitive information or child/young person files should be securely shredded. This also applies to handwritten notes if the notes reference any other staff member or child/young person by name.
- Care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers.
- If information is being viewed on a PC, staff must ensure that the window and documents are properly shut down before leaving the computer unattended. Sensitive information should not be viewed on public computers.
- USB sticks should not be used to transport data away from the establishment.
- No personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party;
- All personal data is kept in accordance with The Witherslack Group retention schedule;
- All staff must keep up to date with the Bring Your Own Device ( BYOD ) guidance incorporated into this policy at Annex 1.

These guidelines are clearly communicated to all establishment staff, and any person who is found to be breaching this conduct will be disciplined in line with the seriousness of their misconduct.

Any queries regarding data protection, including subject access requests and complaints, are promptly directed to the Data Protection Team. Advice is also available on the Witherslack Way.

Any data protection breaches are immediately brought to the attention of the Data Protection Team and that they support the Data Protection Team in resolving breaches.

**A Breach response plan** is available on the intranet. WG have an associated policy namely **Policy Doc – Response Plan – Breach of Data Protection**.

Where there is uncertainty around a Data Protection matter advice is sought from the Data Protection Team on [dataprotection@Witherslackgroup.co.uk](mailto:dataprotection@Witherslackgroup.co.uk).

When members of staff are responsible for supervising Young People doing work which involves the processing of personal information (for example in class projects), they must ensure that those students are aware of the Data Protection Principles, in particular, **the requirement to obtain the data subject's consent where appropriate**.

In a majority of the cases where third party software and internet providers are used to provide educational support to the classroom activities then this would be a legitimate business interest of the school in the provision of education. Consent isn't a prerequisite however there is a requirement for the young people to be aware of the disclosure of their information and the consequences of it.

Staff who are unsure about who are the authorised third parties to whom they can legitimately disclose personal data should seek advice from the Data Protection Team.



## **[d] Third-Party Data Processors**

Where external companies are used to process personal data on behalf of the Witherslack Group responsibility for the legality of sharing, purpose, retention and security of that data, remains with the Witherslack Group.

Where a third-party data processor is used:

- A data processor must be chosen which provides sufficient guarantees about its security measures to protect the processing of personal data;
- Reasonable steps must be taken that such security measures are in place;
- The Data Protection Team must be consulted in writing - [dataprotection@witherslackgroup.co.uk](mailto:dataprotection@witherslackgroup.co.uk);
- A written 'processor' contract establishing what personal data will be processed and for what purpose must be considered;
- All Subject access requests will be forwarded to Our Data Protection Team as soon as they are received - [dataprotection@witherslackgroup.co.uk](mailto:dataprotection@witherslackgroup.co.uk);
- Any Breach in relation to Data protection will be reported to Our Data Protection Team immediately either verbally or by using the notification reporting form sent to [dataprotection@witherslackgroup.co.uk](mailto:dataprotection@witherslackgroup.co.uk).

When staff are implementing any process or system which requires the sharing of personal data, with a third party, they are advised to contact the Data Protection Team who will assist with guidance and support in relation to the implementation.

For further guidance about the use of third-party data processors please contact the Data Protection Team.

## **[e] Contractors, Short-Term and Voluntary Staff**

The Witherslack Group are responsible for the use made of personal data by anyone working on its behalf. Managers who employ contractors, short term or voluntary staff must ensure that they are appropriately vetted for the data they will be processing. In addition managers should ensure that:

- any personal data collected or processed in the course of work undertaken for The Witherslack Group is kept securely and confidentially;
- consideration as to whether their position is as a potential 'Processor' and therefore a third party data processor as above;
- all personal data is returned to The Witherslack Group on completion of the work, including any copies that may have been made. Alternatively that the data is securely destroyed and We receive notification in this regard from the contractor or short term / voluntary member of staff;
- we receive prior notification of any disclosure of personal data to any other organisation or any person who is not a direct employee of the contractor;
- any personal data made available by Us, or collected in the course of the work, is neither stored nor processed outside the EU unless written consent to do so has been received from Us;
- all practical and reasonable steps are taken to ensure that contractors, short term or voluntary staff do not have access to any personal data beyond what is essential for the work to be carried

out properly;

- all Subject access requests will be immediately forwarded to Our Data Protection Team. [dataprotection@witherslackgroup.co.uk](mailto:dataprotection@witherslackgroup.co.uk) (see section 5);
- any Breach in relation to Data protection will immediately reported to Our Data Protection Team. [dataprotection@witherslackgroup.co.uk](mailto:dataprotection@witherslackgroup.co.uk) (see section 7).

#### **[f] Student/Parent responsibilities**

Students are responsible for:

- Ensuring that their personal data provided to the Witherslack Group is accurate and up to date.
- Keeping up to date with the Bring Your Own Device ( BYOD ) guidance incorporated into this policy at Annex 1.

### **5. Requesting Data (Subject Access Request)**

Individuals have the right to access their personal data and supplementary information. The right of access allows individuals to be aware of and verify the lawfulness of the processing.

The right of access only entitles an individual access to their own personal data. They are not entitled to information relating to other people, unless:

- their data also relates to other individuals; or
- they are exercising another individual's right of access on their behalf (for example a parent on behalf of a child or a solicitor on behalf of a client).

This access is available free of charge however we can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive.

We may also charge a reasonable fee to comply with requests for further copies of the same information. This does not mean that you can charge for all subsequent access requests.

The fee will be based on the administrative cost of providing the information.

Under the current Data Protection Legislation including Data Protection Act 2018 and (UK) General Data Protection Regulations 2016, individuals will have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information – we have provided in our privacy notices as previously outlined.

In some cases individuals also have the right to;

- request rectification

- request erasure of the data that is held
- ask for its use to be restricted or
- to object to its processing.

We will seek to verify the identity of the person making the request and the information will be sourced. We will provide the information, redacted in accordance with the current Data Protection Legislation including Data Protection Act 2018 and (UK) General Data Protection Regulations 2016, without delay and at the latest within one month of receipt.

We will be able to extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, We will inform the individual within one month of the receipt of the request and explain why the extension is necessary.

All subject access requests will, without delay in the first instance be referred to the Data Protection Team, Lupton Tower, Carnforth. (see SAR guidance)

This initial request does not need to be made in a formal manner. Be aware it could be made informally;

- During a conversation
- via an email
- contained within a letter
- via a third party.

If you receive a request for information about a young person or colleague whether from the person themselves or from someone acting on their behalf, immediately forward the details to [dataprotection@witherslackgroup.co.uk](mailto:dataprotection@witherslackgroup.co.uk) who will progress the request from there.

## **6. Security of Personal Data**

The current Data Protection Legislation including Data Protection Act 2018 and (UK) General Data Protection Regulations 2016 imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations. Personal data may only be transferred outside of the EU in compliance with the conditions for transfer set out in Chapter V of the (UK) GDPR.

We may transfer personal data where the organisation receiving the personal data has provided us with assurance of adequate safeguards. Individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer.

Adequate safeguards may be provided for by:

- Us having a legally binding agreement between public authorities or bodies;
- Our binding corporate rules (agreements governing transfers made between organisations within in a corporate group);
- Our standard data protection clauses in the form of template transfer clauses adopted by the Commission;
- Our standard data protection clauses in the form of template transfer clauses adopted by a

supervisory authority and approved by the Commission;

- Our compliance with an approved code of conduct approved by a supervisory authority;
- Our certification under an approved certification mechanism as provided for in the (UK) GDPR;
- Our contractual clauses agreed authorised by the competent supervisory authority; or
- Our provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority.

There are circumstances whereby We may continue to transfer personal data out with the above. This is where;

- made with the individual's informed consent;
- necessary for the performance of a contract between the individual and the organisation or for pre-contractual steps taken at the individual's request;
- necessary for the performance of a contract made in the interests of the individual between the controller and another person;
- necessary for important reasons of public interest;
- necessary for the establishment, exercise or defence of legal claims;
- necessary to protect the vital interests of the data subject or other persons, where the data subject is physically or legally incapable of giving consent; or
- made from a register which under UK or EU law is intended to provide information to the public (and which is open to consultation by either the public in general or those able to show a legitimate interest in inspecting the register).

Further information is available on the intranet.

## **7. Breaches of Personal Data**

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

A Personal data breach can include:

- Access by an unauthorised third party;
- Deliberate or accidental action (or inaction) by a controller or processor;
- Sending personal data to an incorrect recipient;
- Computing devices containing personal data being lost or stolen;
- Alteration of personal data without permission;
- Loss of availability of personal data.

In relation to a processor; any Breach of Data protection will be immediately reported to Our Data

Protection Team in line with their agreed processing contract [dataprotection@witherslackgroup.co.uk](mailto:dataprotection@witherslackgroup.co.uk).

Where a Data Protection breach occurs in the Witherslack Group, or is suspected, it must be reported immediately in accordance with Our **Policy document – Response Plan–Breach of Data Protection** and the included APPENDIX 5 - 6 Step guidance which is available on the Witherslack Way.

That guidance states that confirmed or suspected data security breaches must be reported immediately using the Breach Notification Form (1) by email: [dataprotection@witherslackgroup.co.uk](mailto:dataprotection@witherslackgroup.co.uk). The initial notification report can be found on the Witherslack Way.

Should there perceived to be a High Risk of harm to data subjects then the DPO will be contacted immediately. There is a contingency plan outlined in the **Policy document – Response Plan–Breach of Data Protection** should the DPO not be available.

Once informed, the data protection team will assume responsibility to initiate an investigation, identify risk and implement the appropriate mitigation. They will also keep a chronological record of actions, decisions and rationales.

The completed form will help provide the following information for consideration as to levels of risk and further reporting to joint controllers, the Information Commissionaires office and if applicable the data subjects.

The information that will be included in a notification to the ICO is:

- The type of personal data breach; including
- The type and estimated number of individuals affected;
- The type and estimated number of personal data records concerned;
- The name and contact details of a point of contact where further information can be obtained, such as that of the data protection officer (DPO);
- The possible outcomes of the personal data breach; and
- A list of measures taken or being taken to deal with the breach and appropriate measures taken to mitigate any adverse effects.

This reporting process is defined in more detail in the Policy Doc – Response Plan- Breach of data protection (attached to this policy as an Appendix).

## **8. Recording of Activity Processing**

### **Activity**

This is recorded centrally by the data protection team in accordance with Article 30 of the (UK) GDPR 2016. Included in this reporting is the balancing considerations in relation to legitimate business interest and impact assessments.

### **Subject access requests**

This is recorded centrally by the data protection team with full details of the request, replies and redaction considerations. These records are retained in accordance with our retention schedule.

### **Breach of Data Protection**

This is recorded and maintained centrally by the data protection team. The record includes;

- Persons involved / role
- Site
- Date of breach
- Breach category
- Description of breach
- Notified by
- Subject category
- No of subjects
- Consequences
- Risk assessment
- Line manger notifications and updates
- Remedial action
- Regulator informed
- Date ICO informed
- Lessons learnt
- Training needs
- Summary
- Sign off.

This spreadsheet is compliant with ICO guidance on breach recording.

### **Privacy notices**

As outlined in section 3 above.

### **Contact details**

Data Protection Team,  
Lupton Tower,  
Carnforth,  
LA6 2PR

E-mail [dataprotection@witherslackgroup.co.uk](mailto:dataprotection@witherslackgroup.co.uk)

Discipline will be a consideration for any breach of this policy and also when investigating any breach of data protection. Discipline will also be a consideration for failure to recognise and report both a breach of data protection or a subject Access request.

Any discipline considerations will be applied in accordance with the Witherslack Group discipline policy.

**Linked Policy for further reading.....**

IT Systems and Services Acceptable Use policy  
Policy document – Response Plan–Breach of Data Protection  
6 step response plan  
Subject access request - Guidance

## **Data Protection Policy**

### **Appendix A**

#### **BYOD (Bring Your Own Device)**

##### **Summary**

- Members of staff personal devices must not at any time contain Witherslack Group data.
- Members of staff personal devices must not be configured for Witherslack Group email.
- Web based Group email and applications may be used by members of staff on personal devices as long as no Witherslack Group data is stored on the device and you log in each time. This will be facilitated by the provision of “web access” to Group email and applications from the device.
- Young people, specifically those in our residential care, are entitled to use their personal devices as deemed appropriate by their children’s home or school.

##### **Purpose**

The purpose of the BYOD Appendix is to define standards, procedures, and restrictions for end users who have specific and authorised business requirements to access school data from a BYOD connected via a Group wireless network or unmanaged network outside of Witherslack Groups direct control. This applies to, but is not limited to, all BYOD and media that fit the following device classifications:

- Smart Phones iPads/TabletsPDAs
- USBs
- Laptop/notebook/tablet computersMobile/cellular phones
- Home or personal computers used to access enterprise resources
- Any mobile device capable of storing school data and connecting to an unmanaged network

The BYOD Policy applies to any BYOD, hardware and related software that could be used to access school resources when the equipment is not approved, owned, or supplied by Witherslack Group.

The use of a smartphone or other own device in connection with the Witherslack Group is a privilege granted to employees through approval of their management. The Witherslack Group reserves the right to revoke these privileges in the event that users do not abide by the policies and procedures set out below.

##### **Conditions of use**

The following is aimed to protect the integrity of Witherslack Group data and ensure it remains safe and secure under Witherslack Group control.

References to the word “device” below includes, but is not limited to, Android, BlackBerry, iPhone, iPad, tablet, Windows mobile or other smartphones.

Users of BYOD must agree to all terms and conditions in this policy to be allowed access to the Witherslack Group data.

Irrespective of security precautions mentioned here, you are expected to use your device in an ethical



manner and in accordance with Witherslack Group Hand Book and e-Safety Policy.

- Your device must lock itself with a PIN (personal identification number set by you).
- If left idle, your device must automatically activate its PIN after a maximum time-out period of 5 minutes.
- In the event of loss or theft of your device, you must inform Witherslack Group within 3 working days.
- Your device will lock your account after 5 failed login attempts.
- Your device or application will lock every 5 minutes, requiring re-entry of your password.

### **Staff**

Your personal device must not at any time contain Witherslack Group data, this includes being configured for email, files, data or any information relating to the Witherslack Group, it's employees or young people.

Your personal devices may be attached to the Witherslack Group's wireless networks if approved by senior management to enable access to web-based Group email and applications and other such applications as you may wish to access from time to time in accordance with the e-safety Policy and Witherslack Group Handbook.

Web based applications may be used i.e. Web based Witherslack Group email as long as no data is stored on the device and you are required to log in each time to use the service.

A device will not be excluded just because it has a camera.

### **Tampering**

Using your device in ways not designed or intended by the manufacturer is not allowed. This includes, but is not limited to, 'jailbreaking' your BYOD.

By jailbreaking your device you are opening your device up to potential security flaws and remote hacking that may compromise our systems and passwords.

### **Liability**

A personal BYOD can be connected to the Witherslack Group infrastructure or services, but the user is personally liable for their device and carrier service costs. Users of personal smartphones are not eligible (except by prior agreement) for reimbursement of expenses for hardware.

### **Access**

Employees that purchase a device on their own that is not in line with our standard approved device lists may not be able to or allowed to have their devices added to our systems. [It is highly recommended that the employee refer to Witherslack Group IT support to review approved devices.] Furthermore, Witherslack Group reserves the right to disable or disconnect some or all services without prior notification.

## **Young People**

Young people in our care may use their personal devices if deemed appropriate by the school or children's home.

Special consideration should be given to the young people in our residential care in regards to access to their personal devices.

A device will not be excluded just because it has a camera.

If it is not felt appropriate that a young person has his or her own device, the young person's risk assessments should be changed to reflect this decision.

## **Disclaimer**

The Witherslack Group hereby acknowledge that the use of a BYOD in connection with the Witherslack Group's business carries specific risks for which you, as the user, assume full liability. These risks include, but are not limited to, the partial or complete loss of data as a result of a crash of the operating system, errors, bugs, viruses, downloaded malware, and/or other software or hardware failures, or programming errors which could render a device inoperable.

This Appendix supersedes all previous policies or guidance.